UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

DAVID GASSMAN, individually and on behalf of all others similarly situated,	
Plaintiff	
v.	**Civil Action No.** 2:25-cv-176
GUARDIAN CREDIT UNION	**DEMAND FOR JURY TRIAL**
Defendant.	

CLASS ACTION COMPLAINT

Plaintiff, David Gassman, individually, and on behalf of all others similarly situated (hereinafter "Plaintiff") brings this Class Action Complaint against Defendant, Guardian Credit Union ("Guardian" or "Defendant"), and alleges, upon personal knowledge as to his own actions, and upon information and belief as to all other matters, as follows.

INTRODUCTION

1. Plaintiff brings this class action to address Defendant's outrageous, illegal, and widespread practice of disclosing—without consent—the Nonpublic Personal Information[1] and Personally Identifiable Financial Information[2] (together, "Personal and Financial Information") of

[1] The United States Congress defines "nonpublic personal information" as "personally identifiable financial information-- (i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by the financial institution." The Gramm-Leach-Bliley Act, 15 U.S.C.A. § 6809(4)(A) ("GLBA").

[2] "Personally identifiable financial information means any information: (i) A consumer provides to [a financial institution] to obtain a financial product or service from [the financial institution]; (ii) About a consumer resulting from any transaction involving a financial product or service between [a financial institution] and a consumer; or (iii) [a financial institution] otherwise obtain[s] about a consumer in connection with providing a financial product or service to that consumer." 16 C.F.R. § 313.3(o)(1).

Plaintiff and the proposed Class Members to third parties, including Google, LLC ("Google"), Google Tag Manager, Google Analytics, LinkedIn, Qualtrics, Adnxs, DoubleClick, and possibly others (collectively the "Third Parties") (in short, "the Disclosure").

2. Guardian is "one of the largest and most trusted financial resources in the community," offering the ability to "manage your money anywhere" to customers across the United States, including in Wisconsin.[3] To provide these services, Guardian operates and encourages its customers to use its website, https://www.guardiancu.org/ (the "Website"), on which customers can access their account information, access Guardian's financial services, and apply for financial products like credit cards.

3. Despite its unique position as a trusted credit union, Guardian used its Website to blatantly collect and disclose Consumers'[4] and Customers'[5] (collectively, "Customers") Personal and Financial Information to Third Parties uninvolved in the provision of financial services—entirely without their knowledge or authorization. Guardian did so by knowingly and secretly configuring and implementing code-based tracking devices ("trackers" or "tracking technologies") into its Website.

4. Through these trackers, Guardian disclosed and continues to disclose Personal and Financial Information that Customers input into and accessed on Guardian's Website. This

[3] *About Us - Guardian Credit Union*, https://www.guardiancu.org/about-us/ (last visited Jan. 23, 2025) ("*About Us*").

[4] The term "consumer" means "an individual who obtains or has obtained a financial product or service from [a financial institution] that is to be used primarily for personal, family, or household purposes, or that individual's legal representative." 16 C.F.R. § 313.3; 15 U.S.C.A. § 6809(9).

[5] "Customer means a consumer who has a customer relationship with [a financial institution]." 16 C.F.R. § 313.3. The term "time of establishing a customer relationship" shall . . . in the case of a financial institution engaged in extending credit directly to consumers to finance purchases of goods or services, mean the time of establishing the credit relationship with the consumer." 15 U.S.C.A. § 6809.

information includes, without limitation: details from Customers membership applications like Customers' status as new members, details about the banking products that Customers select, features they choose for their accounts, Customers' agreement to the application pre-disclosures, beneficiary information, co-applicant information, and how customers decide to fund their new accounts; banking portal and portal registration information, like when Customers access the banking portal and when Customers register for new portal accounts; and credit card application details like Customers' purpose of application, the specific credit cards that Customers select, co-applicant information, and whether Customers agree with disclosures required for the application.

5. Upon information and belief, Guardian utilized data from trackers to improve and to save costs on its marketing campaigns, improve its data analytics, attract new customers, and generate sales. Guardian benefited from use of Customers' Personal and Financial Information. Guardian further allowed the Third Parties, who are uninvolved in Guardian's provision of financial services, to profit from its Disclosure of Customers' Personal and Financial information. And the Third Parties used Customers' Personal and Financial Information for themselves and disclosed to fourth parties who also profited off of it. Google, for example, will use the data collected from Customers of Guardian to sell ads to fourth parties who will profit off of the use of that information.

6. Customers, like Plaintiff and Class Members, simply do not anticipate that a trusted financial institution will send their Personal and Financial Information to hidden Third Parties (who in turn share with fourth parties), all of whom profit off of it; likewise, when Plaintiff and Class Members used Defendant's Website, they thought they were communicating exclusively with a trusted financial institution.

7. At no time did Guardian disclose to Plaintiff or Class Members that it was sharing their Personal and Financial Information with the Third Parties for third- and fourth-party use. Plaintiff and Class Members never signed a written authorization permitting Defendant to send their Personal and Financial Information to the Third Parties who were uninvolved in the provision of financial services. And Guardian never allowed Plaintiff or Class Members a real opportunity to opt-out of its Disclosure.

8. Defendant owed a variety of duties, including common law, statutory, contractual, and regulatory duties, to keep Plaintiff's and Class Members' Personal and Financial Information safe, secure, and confidential.

9. Furthermore, by obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Personal and Financial Information, Defendant assumed legal and equitable duties to those individuals to protect and safeguard their information from unauthorized disclosure.

10. The statutory and regulatory duties Guardian owed Customers include its obligations under federal law. For example, the GLBA requires that "each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information." 15 U.S.C.A. § 6801. Under this federal law, financial institutions like Guardian are explicitly prohibited from disclosing a Customer's Personal and Financial Information without sufficient advance notification and opt-out opportunity. 15 U.S.C.A. § 6801, *et seq*.

11. Guardian ignored all its duties and obligations, including the GLBA's prohibition, by disclosing Customers' Personal and Financial Information without proper advance notification and opt-out rights as required under the GLBA.

12. Examples of "Personal and Financial Information" included in the GLBA are indistinguishable from the types of information Guardian disclosed to Third Parties, including, among other things: (a) "[i]nformation a consumer provides to [Guardian] on an application to obtain a loan, credit card, or other financial product or service"; (b) "[t]he fact that an individual is or has been one of [Guardian's] customers or has obtained a financial product or service from [Guardian]"; (c) "information about [Guardian's] consumer . . . disclosed in a manner that indicates that the individual is or has been [Guardian's] consumer"; (d) "information that a consumer provides to [Guardian] or that [Guardian] or [its] agent otherwise obtain[s] in connection with collecting on, or servicing, a credit account"; "[a]ny information that a consumer provides to [Guardian] or that [Guardian] or [its] agent otherwise obtain[s] in connection with collecting on, or servicing, a credit account; and (e) "any information [Guardian] collect[s] through an Internet 'cookie' (an information collecting device from a web server)." 16 C.F.R. 313.3(o)(2)(i).

13. Guardian breached common law, statutory, and contractual obligations to Plaintiff and Class Members by, *inter alia*, (i) failing to adequately review its marketing programs and web based technology to ensure its Website was safe and secure; (ii) failing to remove or disengage technology that was known and designed to share Personal and Financial Information; (iii) aiding, agreeing, and conspiring with the Third Parties to intercept communications sent and received by Plaintiff and Class Members; (iv) failing to obtain the written consent of Plaintiff and Class Members to disclose their Personal and Financial Information to Third Parties for Third Party and fourth party use; (v) failing to protect Personal and Financial Information and take steps to block the transmission of Plaintiff's and Class Members' Personal and Financial Information through the use of tracking technology; (vi) failing to warn Plaintiff and Class Members; and (vii) otherwise

failing to design and monitor its Website to maintain the confidentiality and integrity of its customers' Personal and Financial Information.

14. Plaintiff seeks to remedy these harms and brings causes of action of Negligence (Count I); Negligence *per se* (Count II); Invasion of Privacy-Intrusion Upon Seclusion, Wis. Stat. 995.50 (Count III); Invasion of Privacy-Disclosure of Private Facts, Wis. Stat. 995.50 (Count IV); Conversion (Count V); Trespass to Chattel (Count VI); Breach of Confidence (Count VII); Breach of Express and Implied Contract (Count VII); Unjust Enrichment (Count IX); Bailment (Count X); Declaratory Judgment (Count XI); Violation of the Wisconsin Deceptive Trade Practices Act, Wis. Stat. § 100.18(1) ("DTPA") (Count XII); Violation of the Wisconsin Consumer Protection Act, Wis. Stat. § 422.503 ("WCPA") (Count XIII); Violation of the Wisconsin Consumer Protection Act, Wis. Stat. § 423.301 (Count XIV); Misappropriation of an Individual's Personal Identifying Information, Wis. Stat. § 943.201 (Count XV); Violation of Wisconsin's Electronic Surveillance Control Law, Wis. Stat. § 968.27 ("ESCL") (Count XVI); Violation of Wisconsin's Electronic Surveillance Control Law, Wis. Stat. § 968.34 (Count XVII); Violation of the Electronic Communications Privacy Act ("ECPA") 18 U.S.C. §§ 2511(1) (Count XVIII); Violation of the Electronic Communications Privacy Act 18 U.S.C. § 2511(3)(A), Unauthorized Divulgence by Electronic Communications Service (Count XIX); Violation of Title II of the Electronic Communications Privacy Act ("Stored Communications Act") 18 U.S.C. § 2702 (Count XX); and Violation of the Computer Fraud and Abuse Act ("CFAA") 18 U.S.C. § 1030 (Count XXI).

15. Plaintiff brings this action, individually and on behalf of all others similarly situated, for damages and equitable relief.

PARTIES

16. Plaintiff David Gassman is a natural person and citizen of Wisconsin, where he intends to remain. Plaintiff Gassman is Guardian's Customer and is a victim of Defendant's unauthorized Disclosure of Personal and Financial Information.

17. Defendant Guardian is a non-federal credit union organized and existing under the laws of the State of Wisconsin, with a principal place of business located at 7801 S Howell Ave., Oak Creek, WI 53154.[6]

18. Guardian's Registered Agent for Service of Process is Kevin Nitka.[7]

19. Guardian is a financial institution, as that term is defined by Section 509(3)(A) of the GLBA, 15 U.S.C. § 6809(3)(A).

20. Guardian has corporate offices in Wisconsin, and maintains physical locations in the state of Wisconsin.[8]

JURISDICTION AND VENUE

21. This Court has personal jurisdiction over Defendant because Defendant operates, conducts, engages in, or carries on a business in this State; it maintains corporate offices in this state; and committed tortious acts in this State.

22. This Court has subject matter jurisdiction under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than one hundred (100) members in the proposed Classes, and at least one member of the Classes is a citizen of a state different from Defendant.

[6] *See Guardian Credit Union*, National Credit Union Service Organization Search, available at https://ncuso.org/credit-union/66638/ (last visited Jan. 23, 2025).

[7] *Id.*

[8] *Id.*; *see generally* the Website.

23. This Court also has subject matter jurisdiction under 28 U.S.C. § 1331 because it arises under the laws of the United States. The Court has supplemental jurisdiction over Plaintiff's claims arising under state law pursuant to 28 U.S.C. § 1367.

24. Venue is proper under 28 U.S.C. § 1391(b)(2) because a substantial part of the events and omissions giving rise to Plaintiff's claims occurred in this District and continue to occur in this District.

COMMON FACTUAL ALLEGATIONS

A. Guardian Collects Personal and Financial Information Under the Guise of Protecting it

25. Guardian services its customers through its Mobile and Online Banking, which allows Customers to "manage [thei]r money anywhere."[9] "Guardian Credit Union is committed to providing a website that is as accessible as our branches."[10]

26. Guardian assures Customers that it "Maintain[s] the confidentiality of member information which you provide to us."[11]

27. Guardian portrays its commitment to privacy to its Customers:[12]

[9] *See About Us*; *Online & Mobile Banking*, https://www.guardiancu.org/online-mobile-banking/ (last visited Jan. 23, 2025) ("*Online & Mobile Banking*").

[10] *Privacy Policy*, https://www.guardiancu.org/privacy-policy/(last visited Jan. 23, 2025) ("*Privacy Policy*") (attached as Exhibit A).

[11] *Id.*

[12] *Id.*

Online privacy policy

Guardian Credit Union respects your right to privacy. When you visit our website, you may be providing information to Guardian Credit Union on two different levels: anonymous statistics collected as you browse the site and personal information you knowingly give us.

Security of your information

Guardian Credit Union would like to assure you that we **do not**:

- Collect personal information from you unless you provide it to us, or
- Sell the names and addresses of our members and site users to outside parties.

Guardian Credit Union **does**:

- Safeguard members' and site users' information from unauthorized access, and
- Maintain the confidentiality of member information which you provide to us.

28. Defendant serves its Customers via its "online and mobile banking," encourages customers to use its Website to, for example, learn about Guardian and its services,[13] view financial and educational resources,[14] join Guardian Credit Union,[15] apply for and access savings and checking accounts,[16] apply for and access checking accounts and debit cards[17] compare Guardian's credit card offers,[18] apply for credit cards,[19] apply for loans including mortgages, personal loans, and student loans,[20] enroll in online banking,[21] access online banking,[22] and much more.[23]

[13] *See generally*, *Online & Mobile Banking* and *About Us*.

[14] *See Financial Resources*, https://www.guardiancu.org/resources/ (last visited Jan. 23, 2025).

[15] *See generally,* the Website; *Membership & Services*, https://www.guardiancu.org/membership-and-services/ (last visited Jan. 23, 2025).

[16] *See Savings Accounts*, https://www.guardiancu.org/savings-and-checking/savings-accounts/ (last visited Jan. 23, 2025).

[17] *See Guardian Visa Debit Card*, https://www.guardiancu.org/debit/ (last visited Jan. 23, 2025).

[18] *See Guardian Visa Credit Cards*, https://www.guardiancu.org/loans/credit-cards/ (last visited Jan. 23, 2025) ("*Credit Cards*").

[19] *Id.*

[20] *See Loans*, https://www.guardiancu.org/loans/ (last visited Dec. 16, 2024).

[21] *Online & Mobile Banking*.

[22] *Id.*

[23] *See generally* the Website.

29. In short, Defendant encourages customers to use its Website to "manage your money anywhere."[24]

30. Defendant promotes the comprehensive functionality and use of its Website in service of its own goal of increasing profitability. In furtherance of that goal, Defendant purposely and secretly installed the Third Parties' online tracking technology onto its Website to gather information about Customers.

31. Guardian utilized the information it collected to market its services and bolster its profits by surreptitiously diverting the information to Third Parties like Google.

32. But Defendant did not only collect information for its own use; Guardian also shared—and continues to share—Customers' information, including Personal and Financial Information, with the unauthorized Third Parties who then use it for their own benefit and to benefit fourth parties who are even further removed from the Customers.

B. Third Parties and Trackers: Collectors and Profiteers of Personal and Financial Information

33. The invisible Third Party online tracking technologies installed by Guardian on its Website gathers a vast assortment of Customer data. The installation of these trackers—and thus their transmission of data—is in Guardian's exclusive control.

34. When an individual accesses a webpage containing online tracking technology from a Third Party, the trackers instantaneously and surreptitiously duplicate communications with that webpage and send them to the Third Party. The information travels directly from both the Customer's browser and the webpage owner's server and then on to the Third Party's server, based off instructions from the Third Party's tracker. The communications and information transmitted via these trackers are entirely in Defendant's control; Customers trust Guardian with the

[24] *See About Us*.

information they input on Guardian's Website, and Guardian is in complete and exclusive control of its Website and the data input therein. The transmission of Customers' data only occurs on webpages that contain tracking technology.

35. Online tracking technologies may not be deleted from an individual's device; they are built into a webpage, and a webpage Customer has no control or warning over their presence or data collection. Third party trackers cause information to flow directly from the website Customer's browser and the website owner's server to the Third Party itself. A webpage Customer cannot prevent or even detect this transmission of data.

36. Accordingly, without any knowledge, authorization, or action by a Customer, a website owner who has installed Third Party trackers is utilizing website source code to commandeer its Customers' computing devices and web browsers, causing them to invisibly re-direct the Customers' communications to Third Parties.

37. In this case, Defendant employed the Third Party trackers to intercept, duplicate, and re-direct Plaintiff's and Class Members' Personal and Financial Information to the Third Parties contemporaneously, invisibly, and without the customer's knowledge.

38. Consequently, when Plaintiff and Class Members visited Defendant's Websites and communicated their Personal and Financial Information, that information was simultaneously intercepted and transmitted to the Third Parties.

39. The Third Party trackers do not provide any substantive content on Guardian's Website. Rather, their only purpose is to collect information to be used for the Third Party and fourth parties' marketing and sales purposes.

40. The Google trackers allow Defendant to track and share with Google (1) who uses Guardian's Website; (2) what is performed on the Website; (3) when Customers visit the Website;

(4) where on the Website Customers perform these actions; and (5) how Customers navigate through the Website to perform these actions. Google gathers this information using trackers embedded on Guardian's Website and generates corresponding reports.[25] Google Tag Manager, Google Analytics, and DoubleClick are part of the suite Google uses to collect all of this.[26] Google's collection of this data "enables advertisers to more effectively create, manage and grow high-impact digital marketing campaigns."[27]

41. Furthermore, on information and belief, Defendant utilized LinkedIn trackers. "LinkedIn analytics is a collection of metrics that measure the effectiveness of your posts, updates and strategy on the platform. It's statistical data that enhances your LinkedIn marketing efforts."[28]

42. Qualtrics is another tracker Defendant uses. Qualtrics collects "mountains of data" and analyzes it using Artificial Intelligence.[29]

43. And Defendant utilizes Adnxs, which is a cookie that tracks online activity an displays targeted ads. It can operate as a virus or malicious program, redirecting the browser to unwanted and unintended pages, programs, malware, or other intrusive and potentially harmful content.[30]

C. Guardian Used Trackers to Unauthorizedly Disclose Personal and Financial Information

---

[25] *See generally*, *A big list of what Google Analytics can & cannot do*, MarketLytics, avail. at https://marketlytics.com/blog/list-of-things-google-analytics-can-and-cannot-do/.

[26] *See the DoubleClick Digital marketing Suite,* Google Developers, https://developers.google.com/app-conversion-tracking/third-party-trackers/doubleclick (last visited Aug. 8, 2024).

[27] *See DoubleClick Digital Marketing*, Google Help, https://support.google.com/faqs/answer/2727482?hl=en (last visited June 26, 2024).

[28] SproutSocial, Rana Bano, March 5, 2024, *LinkedIn analytics: The complete guide for tracking metrics in 2024,* avail. at https://sproutsocial.com/insights/linkedin-analytics/ (last acc. Aug. 8, 2024).

[29] *See Qualtrics*, https://www.qualtrics.com/ (last visited Jan. 23, 2025).

[30] *See How To Remove Adnxs.com Redirect [Virus Removal Guide]*, https://malwaretips.com/blogs/ib-adnxs-popup-virus/ (last visited Jan. 23, 2025).

44. On information and belief, Guardian installed each of these trackers, through which Guardian transmitted Customers' communications with Guardian's website and thus their Personal and Financial Information to the Third Parties without Customers' knowledge or authorization. Guardian reports information to the Third Parties when Customers apply for (i) a Guardian membership, (ii) portal accounts, and (iii) credit cards, informing third parties about Customers' progression through the applications, and specific details including personally identifiable information that Customers provide to Guardian as part of the application processes.

45. On information and belief, since at least September 6, 2017, and at least as recently as November 6, 2024, Guardian has tracking technologies installed on its Website.

46. Accordingly, Guardian disclosed its Customers'—including Plaintiff's and the Class Members'—data and Personal and Financial Information to the Third Parties, like Google, beginning at or before September 6, 2017, and at least up to November 6, 2024.

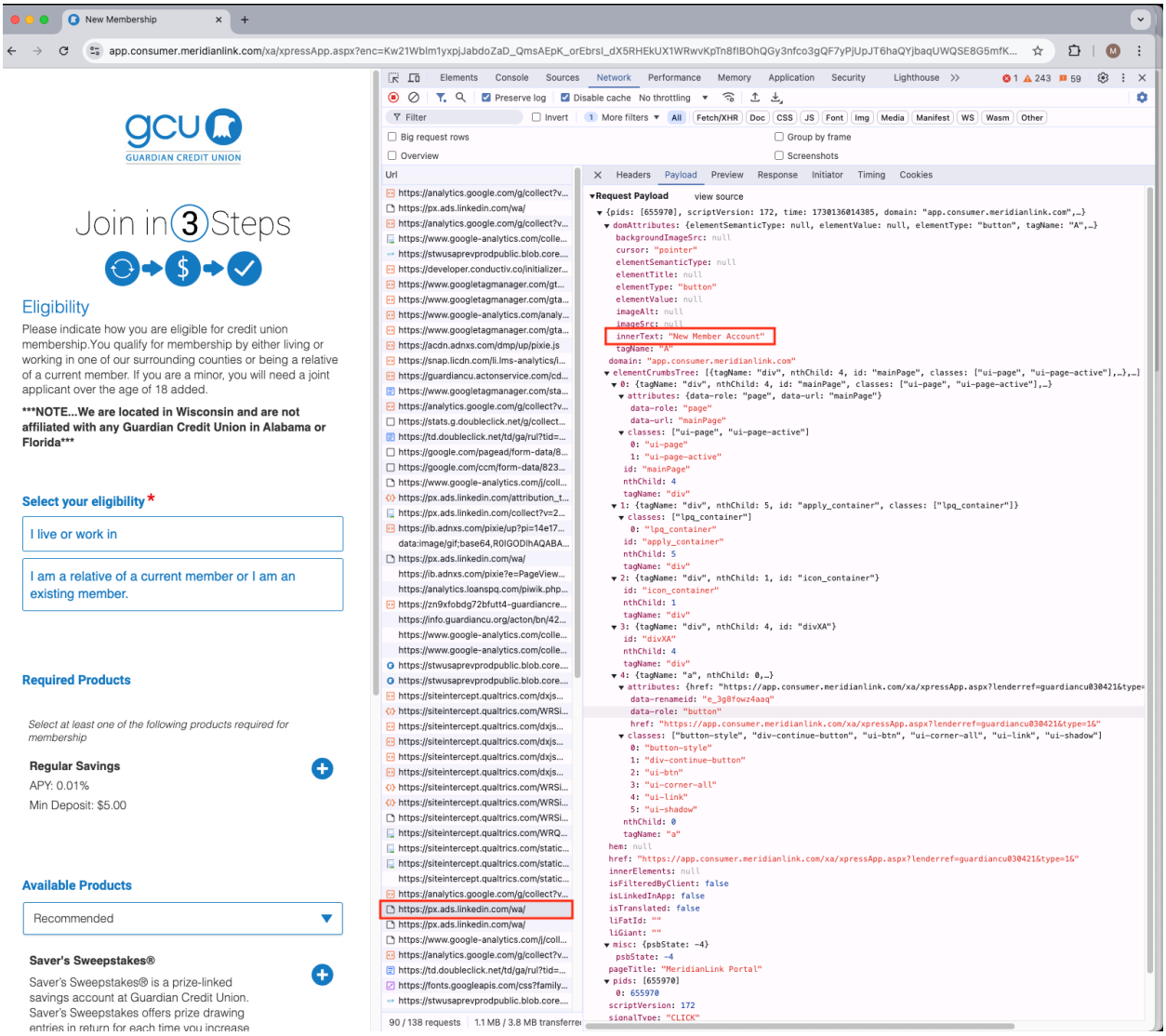
47. By way of example, as configured as of November 6, 2024, Defendant's Google trackers and/or its other tracking technologies, disclosed significant information to Third Parties including Google.

i. Guardian Installed Google Trackers to Track Guardian's Membership Application Information.

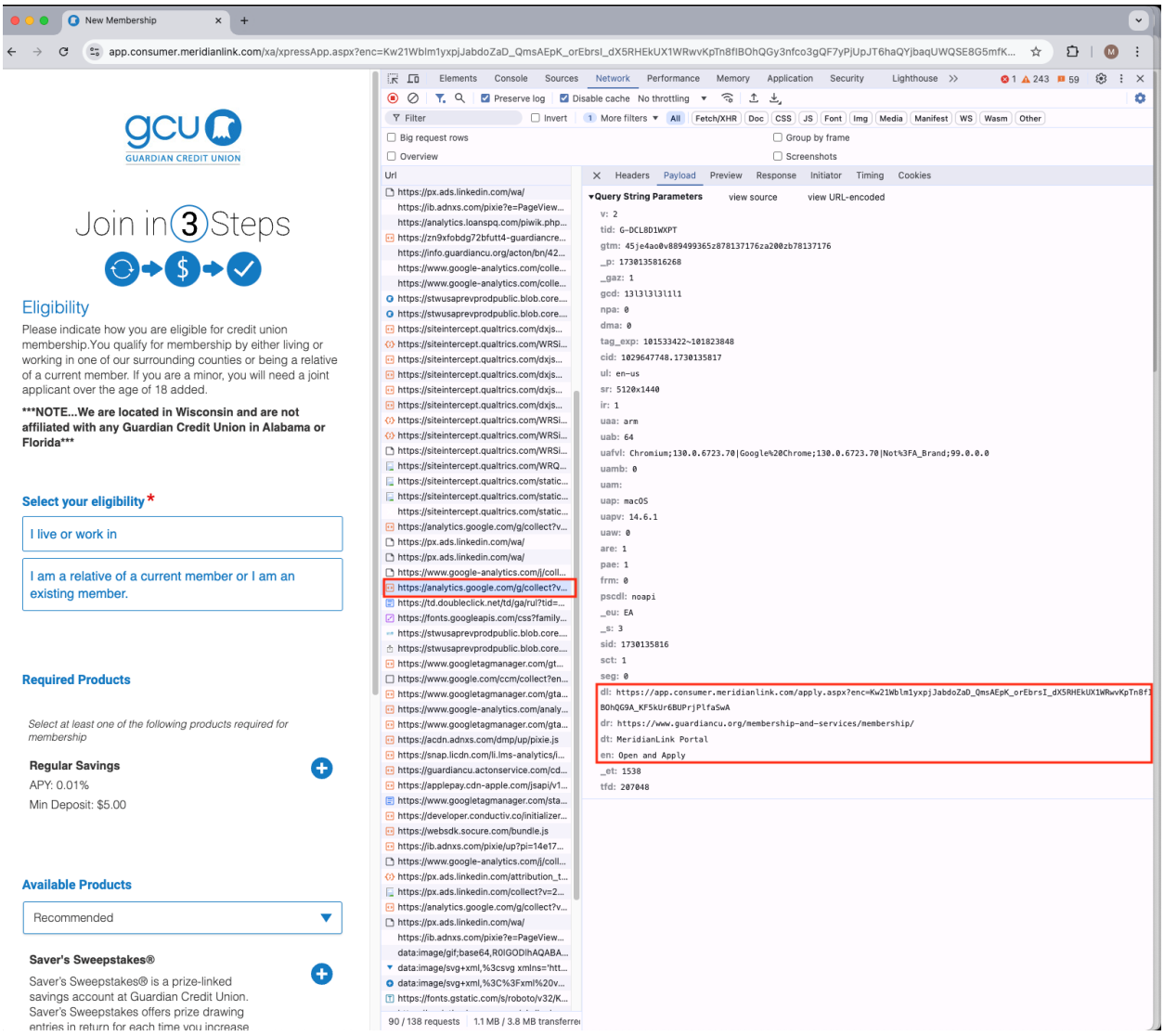
48. Guardian shares with third parties, Customers' status as new members and details from Customers' membership applications, including (i) details about the banking products that Customers select and features that Customers choose for their accounts; (ii) Customers' agreement to the application pre-disclosures; (iii) whether Customers have beneficiaries or co-applicants; and (iv) how Customers decide to fund their new accounts.

49. When a Customer fills out a membership application, Guardian sends events to the following third parties, indicating that the Customer is a new member:

a. LinkedIn, providing that the Customer selected for “New Member Account”:

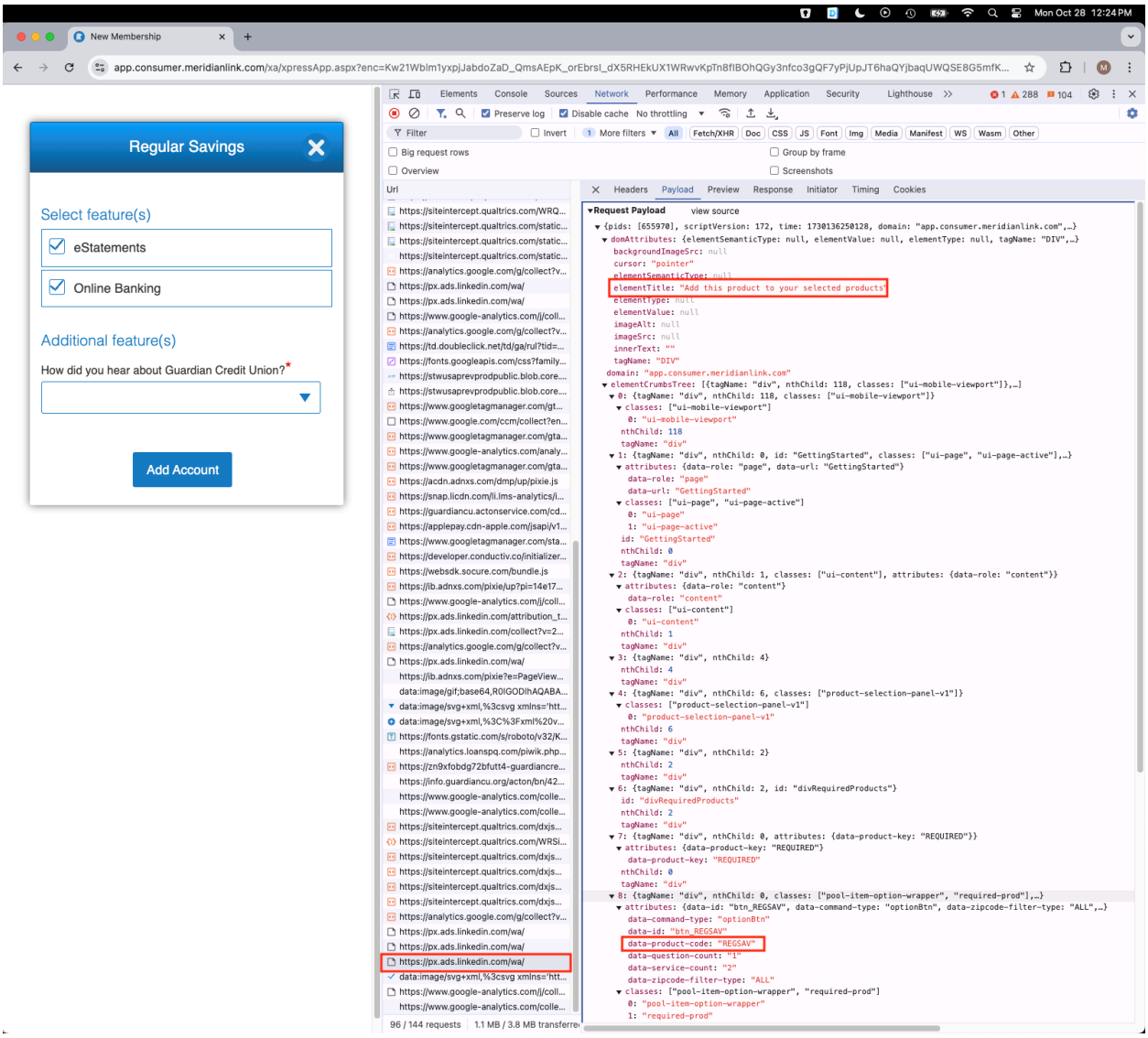


b. Google, providing that the Customer is on the page for Guardian's "membership-and-services/membership," through an "Open and Apply" event, or that the Customer is on a page for "New Membership" through pageview events:

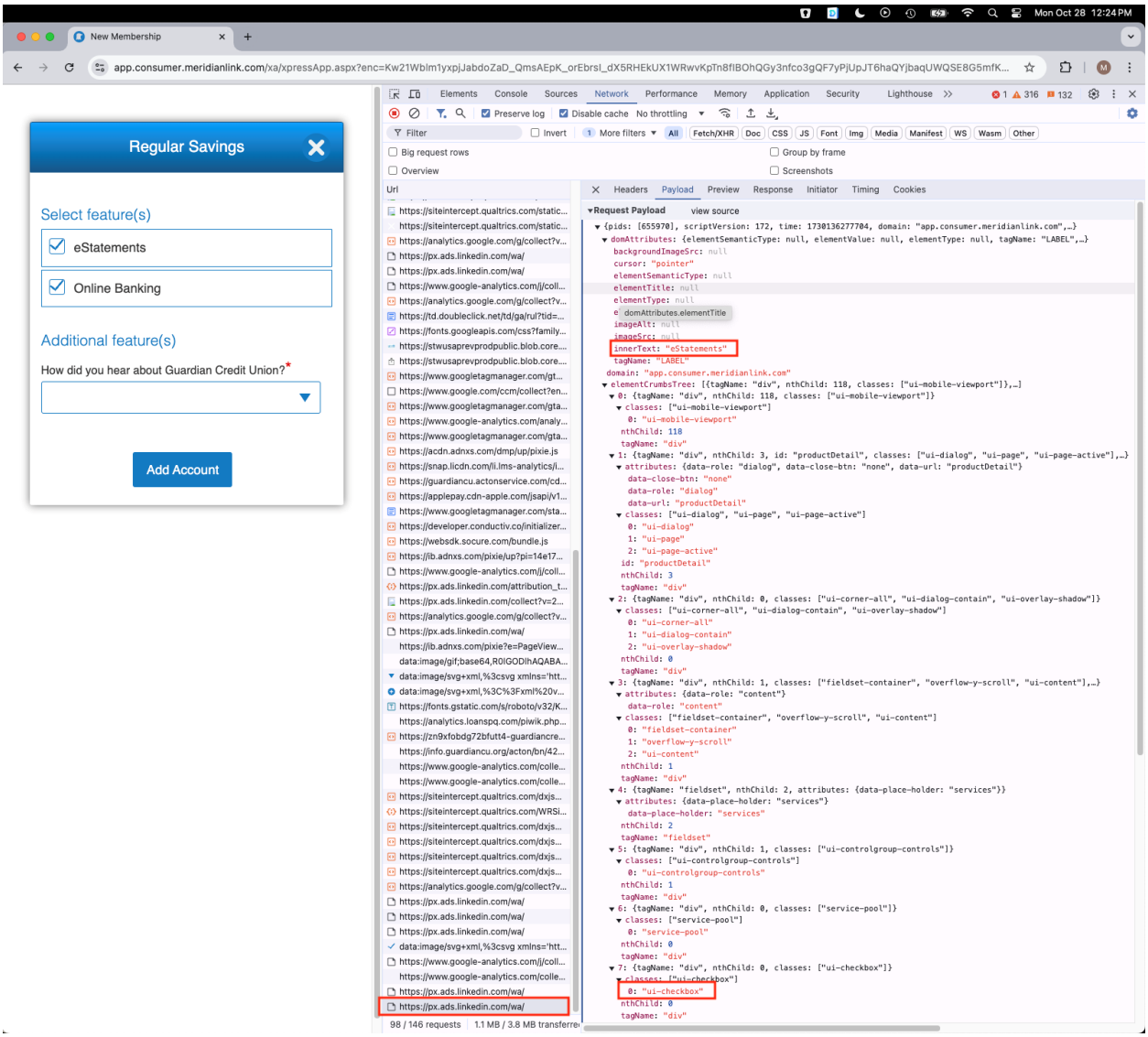


50. Additionally, Guardian shares information with third parties about Customer' choices from their new membership applications.

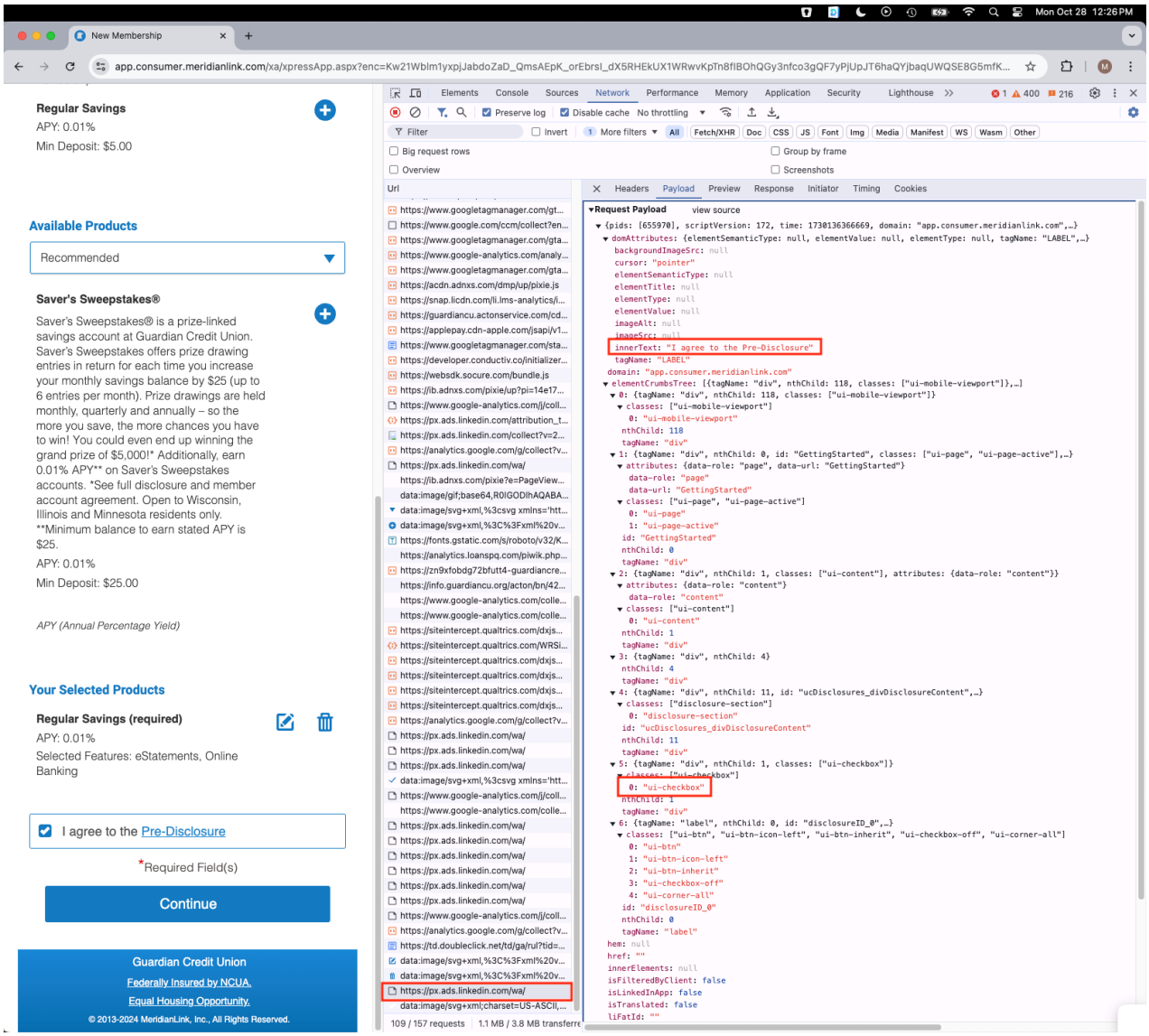
51. For example, Guardian reports the type of banking product that Customers select. If a Customer chooses regular savings for their desired banking product, Guardian reports to LinkedIn and Google that the Customer selected "REGSAV."



52. Similarly, Guardian discloses features that Customers choose for their account. For instance, when a Customer chooses to add eStatements as a feature to their account, Guardian reports to LinkedIn that the Customer selected "eStatements."

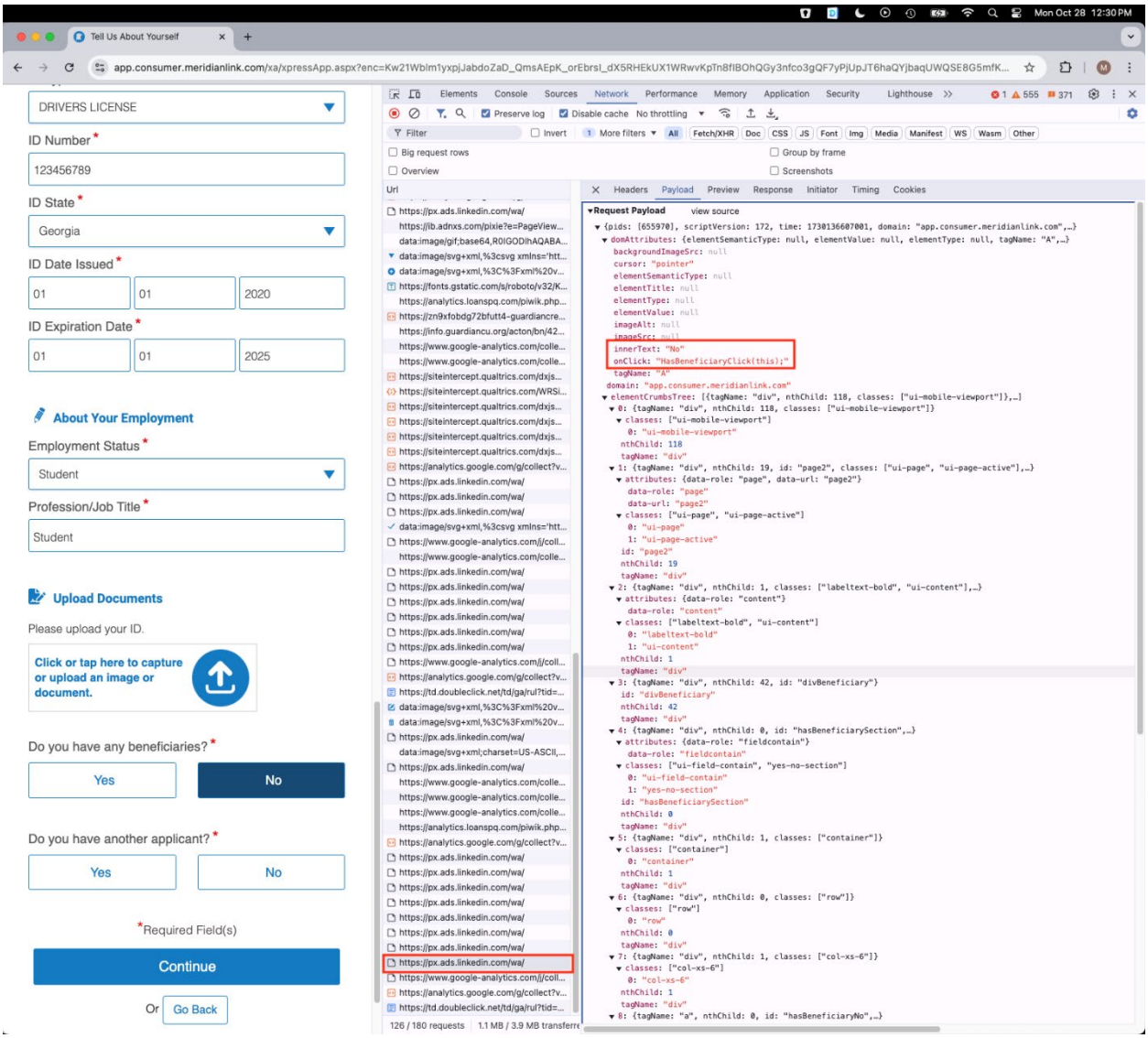


53. Moreover, when a Customer agrees to Guardian's pre-disclosures, Guardian reports the Customer's agreement to LinkedIn, providing that the Customer selected "I agree to the Pre-Disclosure."

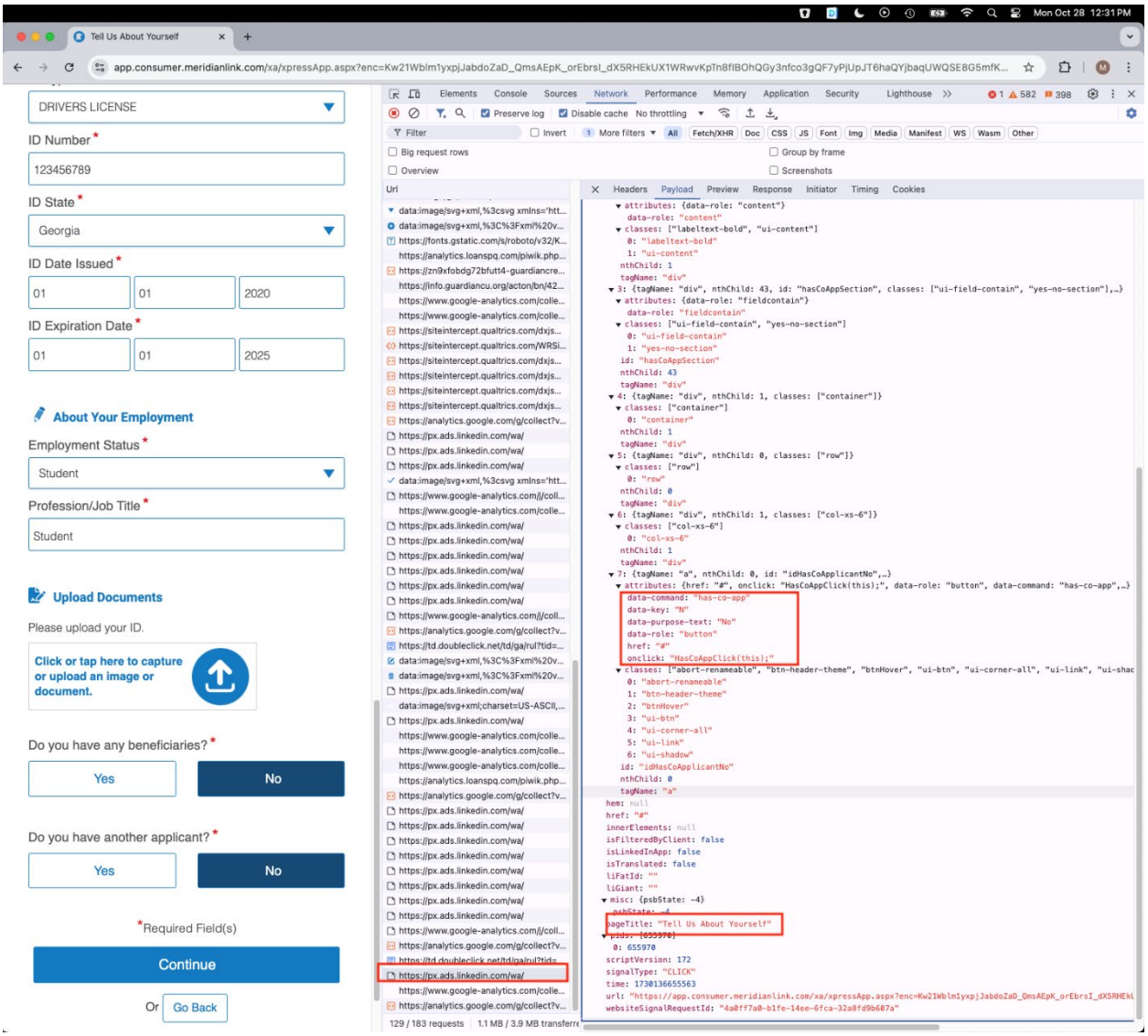


54. Guardian also discloses whether Customers have any beneficiaries or co-applicants.

55. To illustrate, when a Customer indicates that they do not have a beneficiary, Guardian transmits an event to LinkedIn, reporting that the Customer selected "No," in response to whether the Customer "has-beneficiary."



56. When a Customer selects that they do not have any co-applicants, Guardian would likewise send an event to LinkedIn, indicating that the Customer selected "idHasCoApplicantNo."



57. Guardian also reports to LinkedIn and Google the method by which Customers choose to fund their new accounts.

58. Such as when a Customer chooses to fund their new account by credit card, Guardian first sends an event to LinkedIn indicating that the Customer selected "I agree to fund the account(s) with the method selected," as well as another event indicating that the Customer selected the option, "Credit Card," from the "funding-option-lst."

59. Once the Customer arrives on the page to input their credit card information in order to fund their new account, Guardian sends events to LinkedIn, providing that the Customer is on a page which collects information from the Customer for "fundingCreditcard."

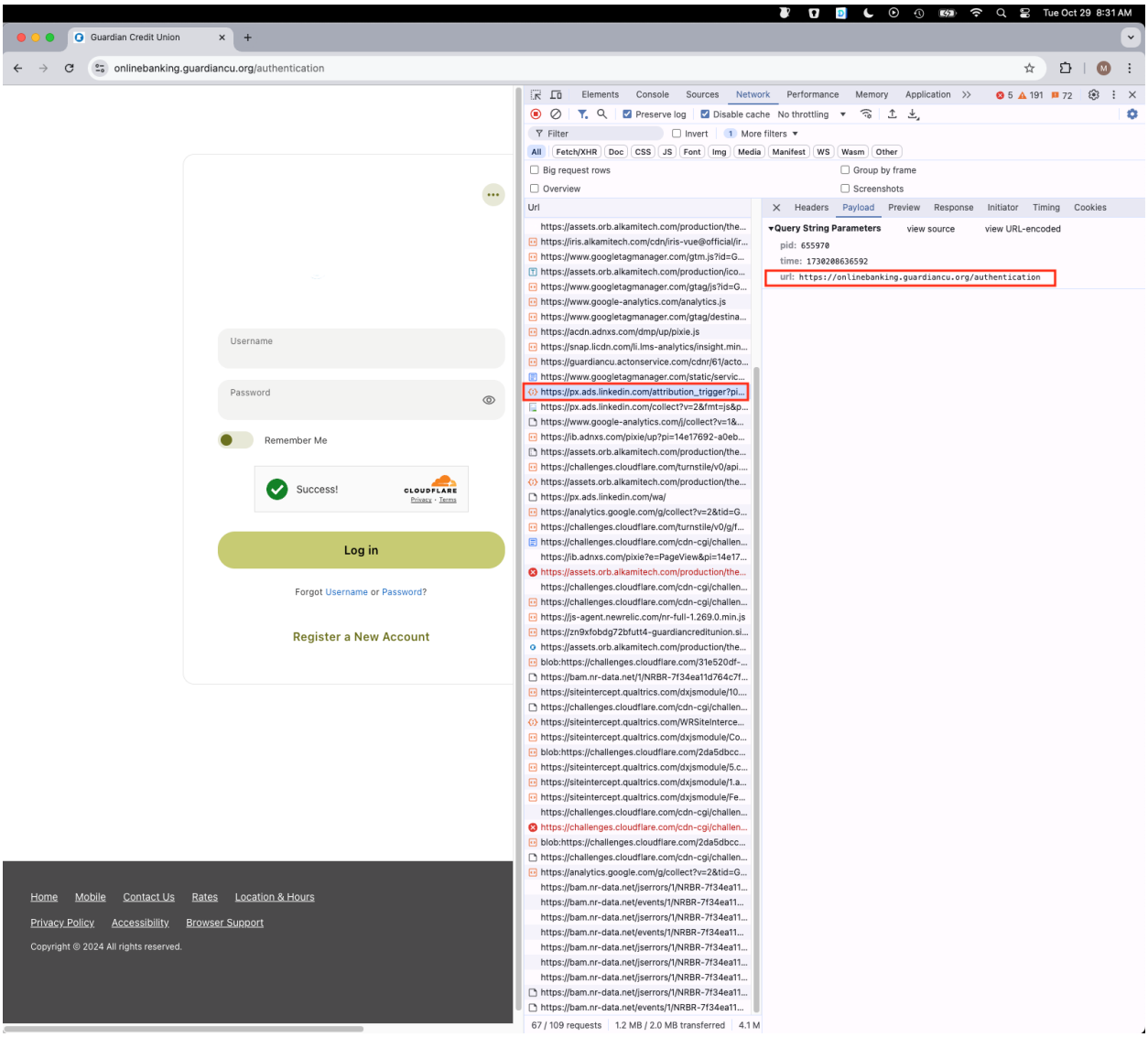
60. Guardian also sends two events to Google, informing it about the Customer's choice to fund their new account via credit card, with one event indicating that the Customer selected "Credit Card" on a page titled "Funding," and another event indicating that the Customer chose to "Fund via Credit Card."

61. If the Customer instead choses to fund an account by check, Guardian would inform LinkedIn and Google about the Customer's selection, indicating to LinkedIn that the Customer selected "Mail a Check," from the "funding-option-lst," and to Google that the Customer selected "Mail A Check."

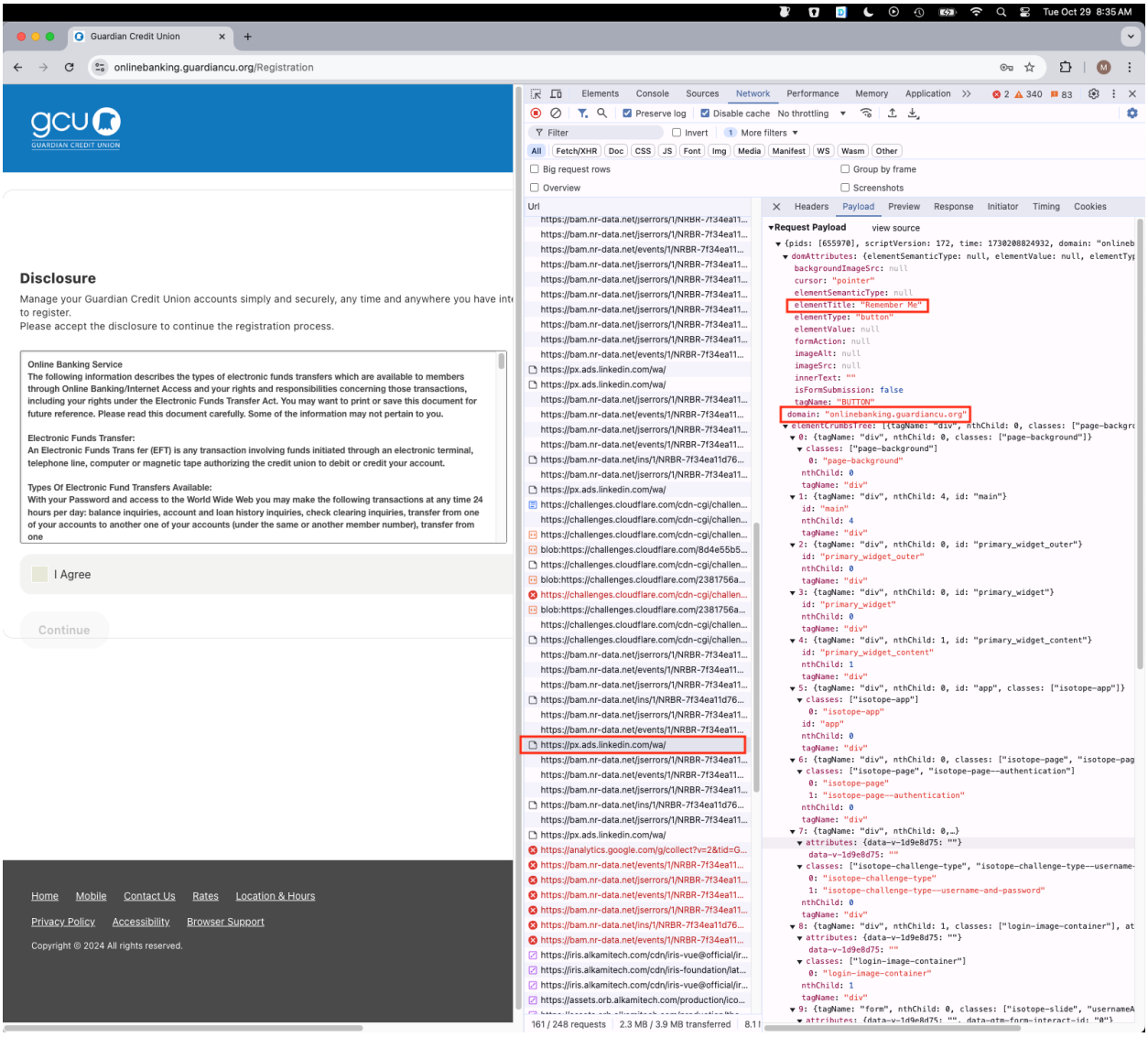
ii. Guardian Installed Google Trackers to Track Guardian's Banking Portal and Portal Registration Information.

62. Guardian informs third parties when users access the banking portal and when users register for new portal accounts.

63. To start, Guardian reports when users load the banking portal page. As a user arrives on the banking portal authentication page, Guardian sends events reporting that the user is viewing the page, "onlinebanking.guardiancu.org/authentication," to LinkedIn and Google.

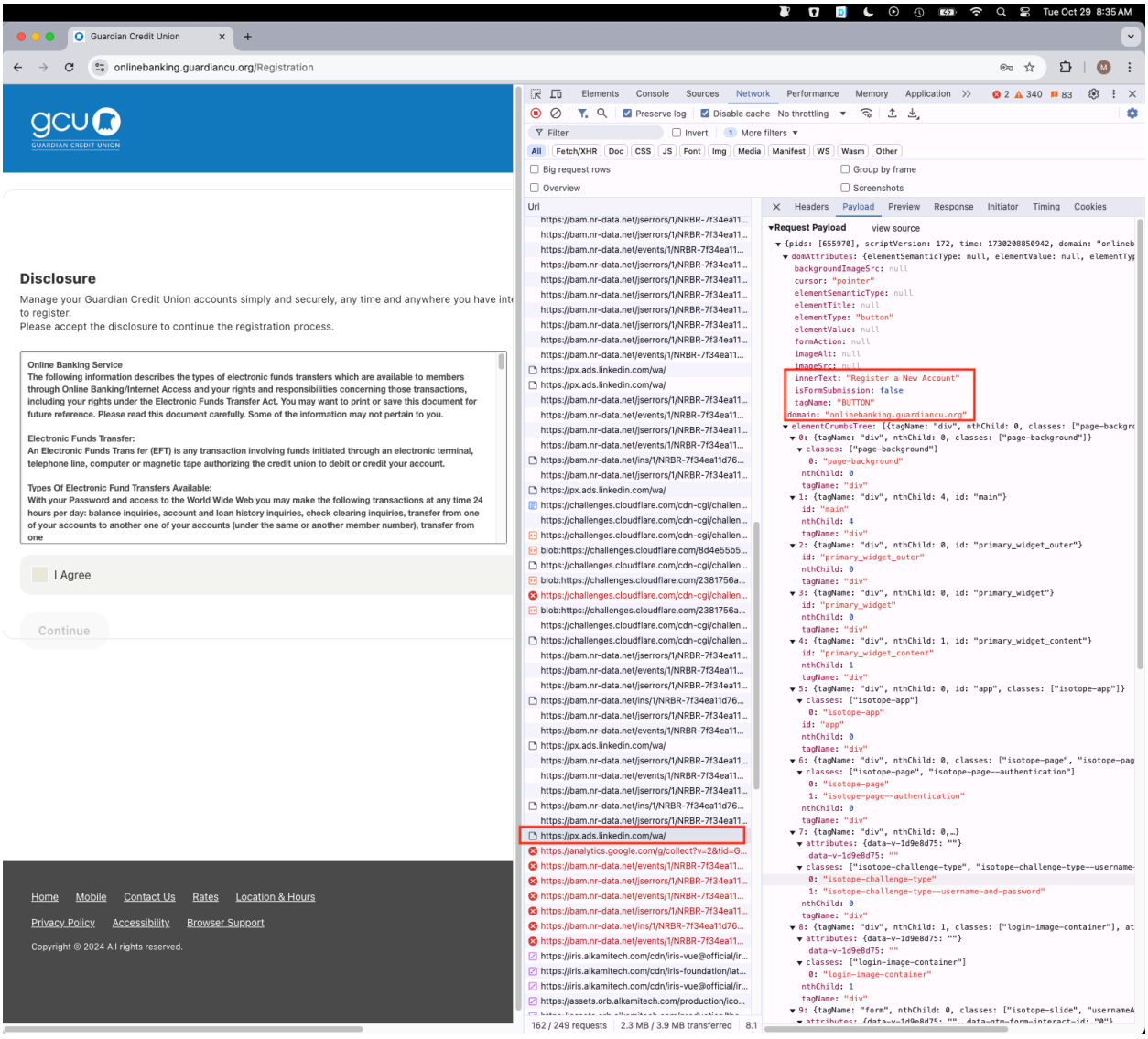


64. Guardian additionally informs LinkedIn when a user selects the option for the site to remember their login information.

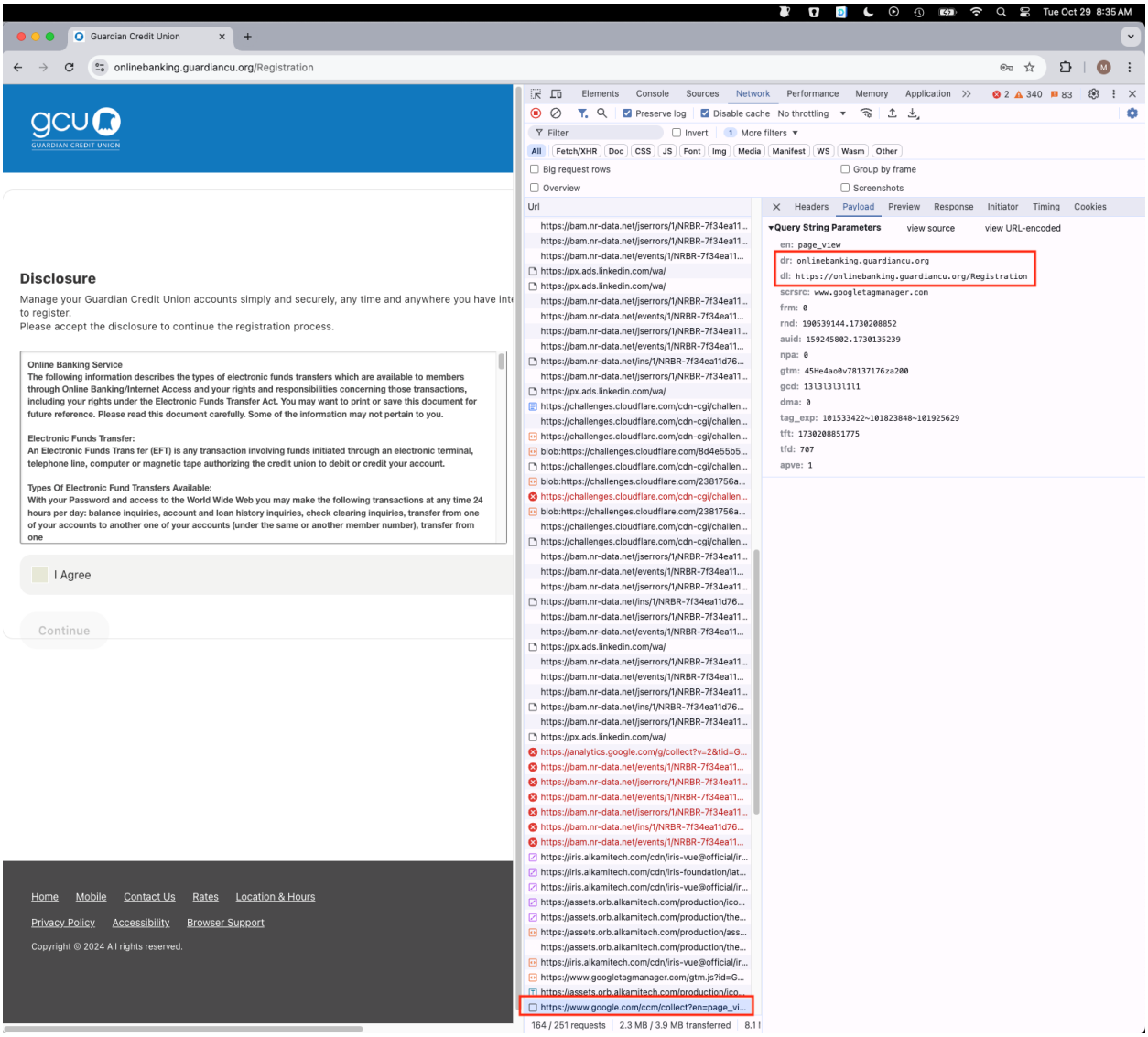


65. Users who do not have an existing banking portal account could register for a new account from the banking portal page. When a user does so, Guardian informs third parties about the user's registration, sending events to:

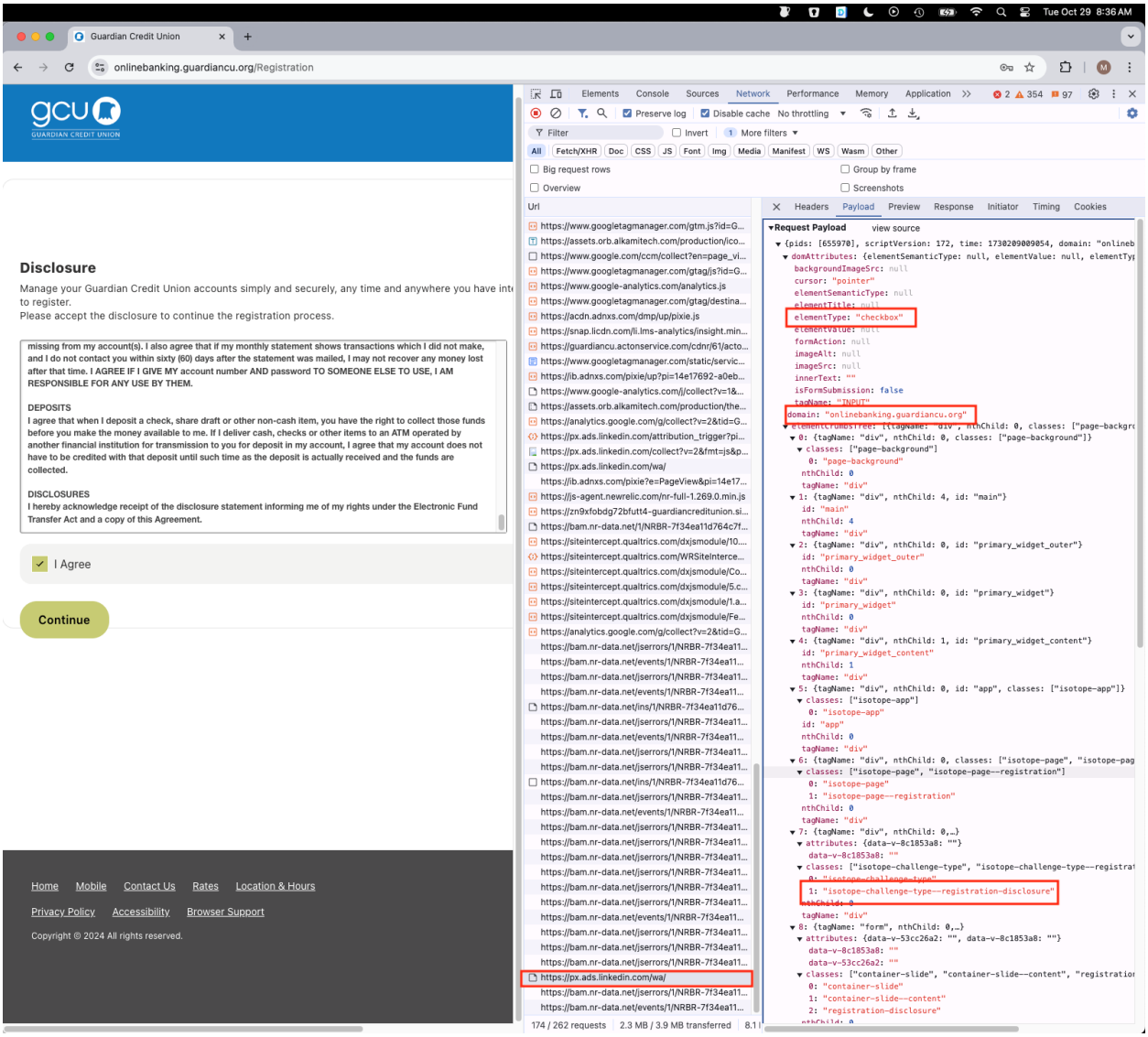
a. LinkedIn, reporting that that the user clicked to "Register a New Account" while they are on the "onlinebanking.guardiancu.org" site; and



b. Google, reporting that the user is on the page "onlinebanking.guardiancu.org/registration."

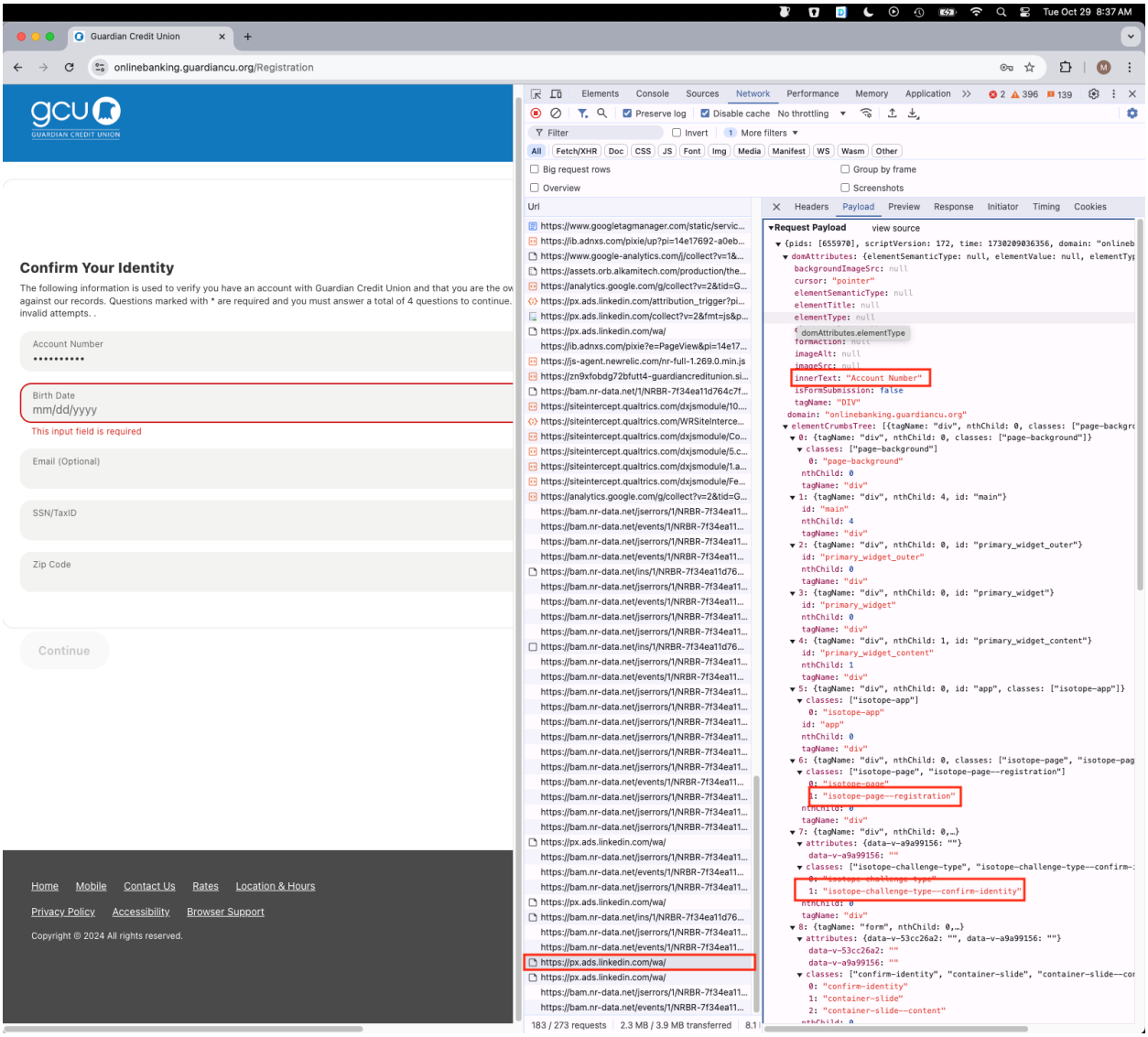


66. As a condition to a user's new registration, Guardian requires that the user accepts a set of disclosures. When a user selects that they agree to the disclosures, Guardian informs LinkedIn that the user selected "accept-disclosure—checkbox" for the "registration-disclosure."

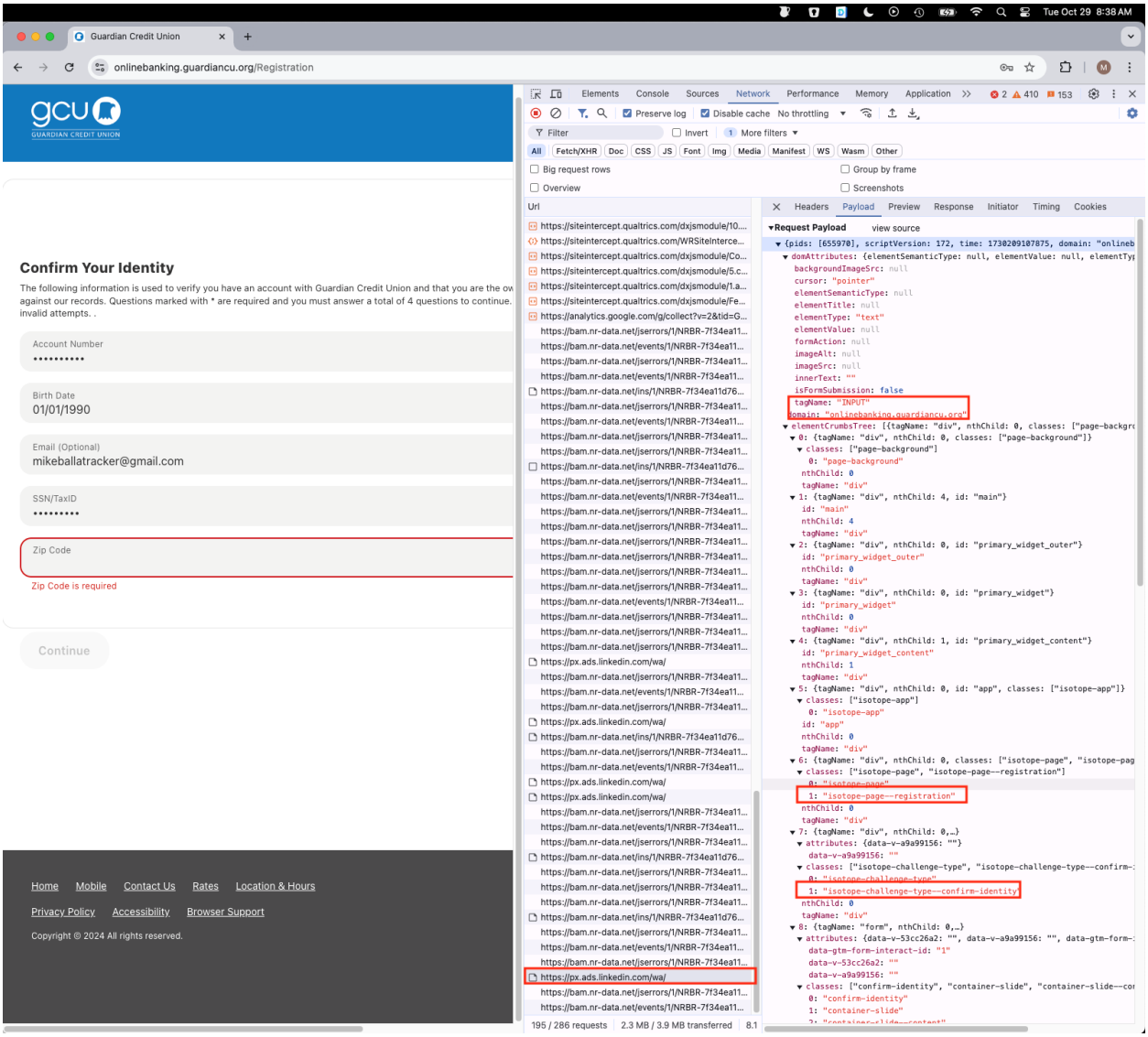


67. Guardian also shares with LinkedIn the type of information that users provide during the application.

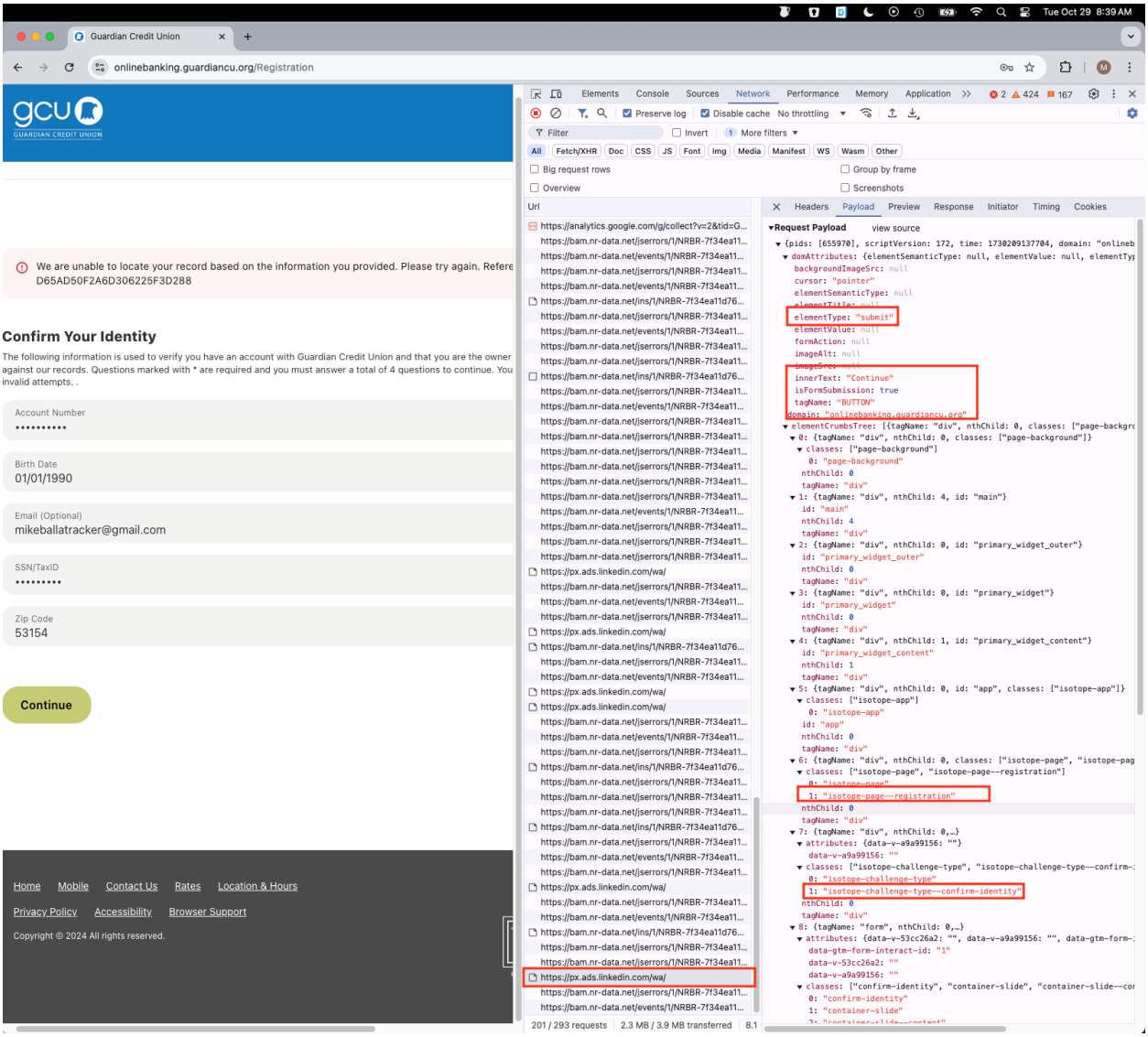
68. For example, a user completing the portal registration must confirm their identity by providing their Guardian account number and zip code. As a user provides their account number, Guardian informs LinkedIn that the user is completing a registration form to "confirm-identity" and that the user selected the portion of the form to input their "Account Number."



69. Likewise, when a user clicks on the application field to provide their zip code, Guardian informs LinkedIn that the user selected the "UserIdentifyingField_ZipCode," while they are on the "onlinebanking.guardiancu.org" website.



70. Next, as the user clicks to proceed to their identity confirmation page, Guardian continues to keep LinkedIn apprised, revealing that the user "CLICK[ed]" a button to "submitConfirmIdentity," while they are on the "onlinebanking.guardiancu.org."

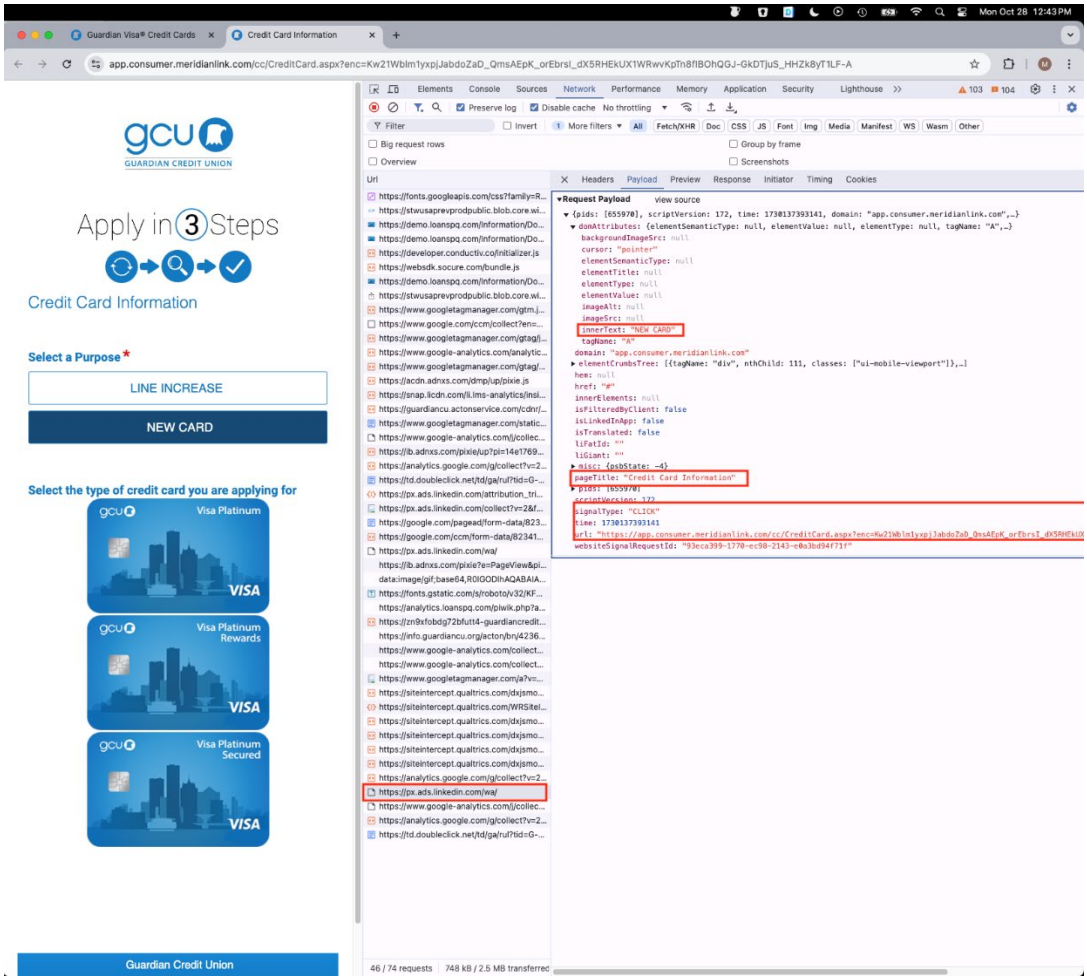


iii. Guardian Installed Google Trackers to Track Guardian's Credit Card Application Information.

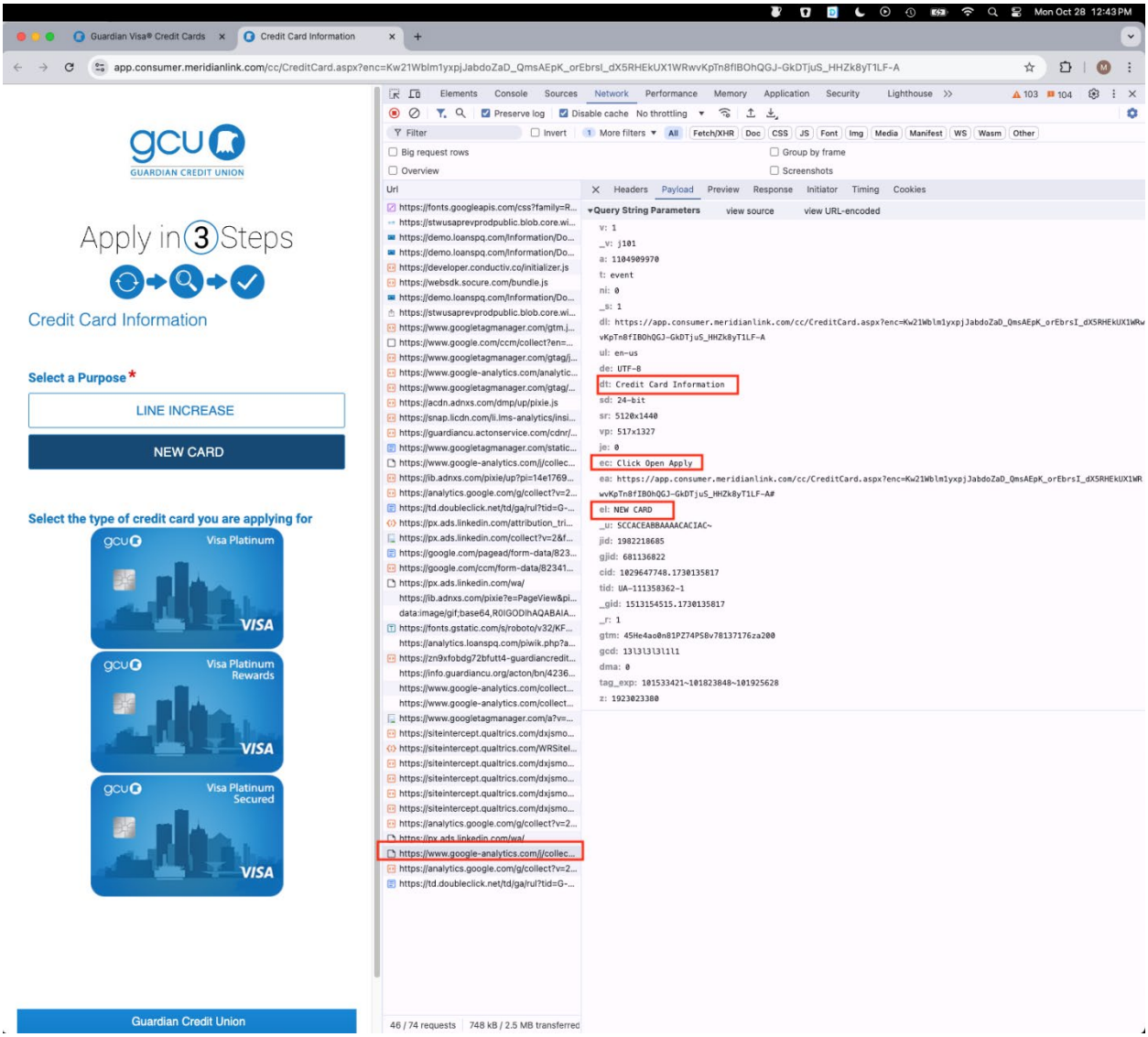
71. Finally, Guardian reports details from users' credit card applications to third parties, sharing: (i) users' purpose of application; (ii) the specific credit cards that users select; (iii) whether users have co-applicants; and (iv) whether users agree with disclosures required for the application.

72. When a user begins their credit card application, Guardian prompts them to select whether they would like a new credit card or a line increase. Guardian reports users' selections to LinkedIn and Google.

73. For instance, if a user is applying for a new credit card, Guardian sends an event to LinkedIn reporting that the user clicked for a "NEW CARD" as their "loan-purpose" while they are on a page called "Credit Card Information."

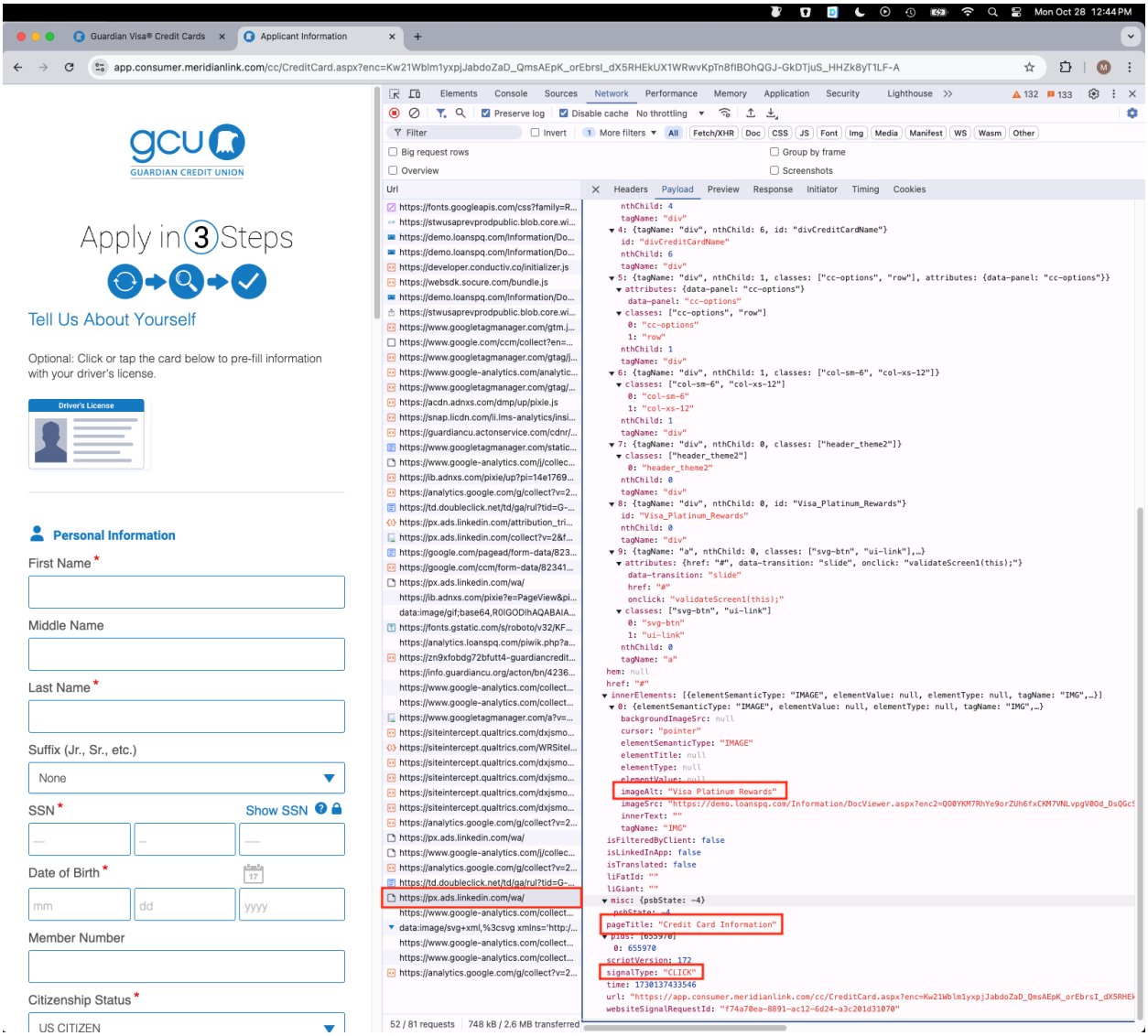


74. Likewise, Guardian informs Google that the user selected the link for "NEW CARD" on the page, "Credit Card Information."

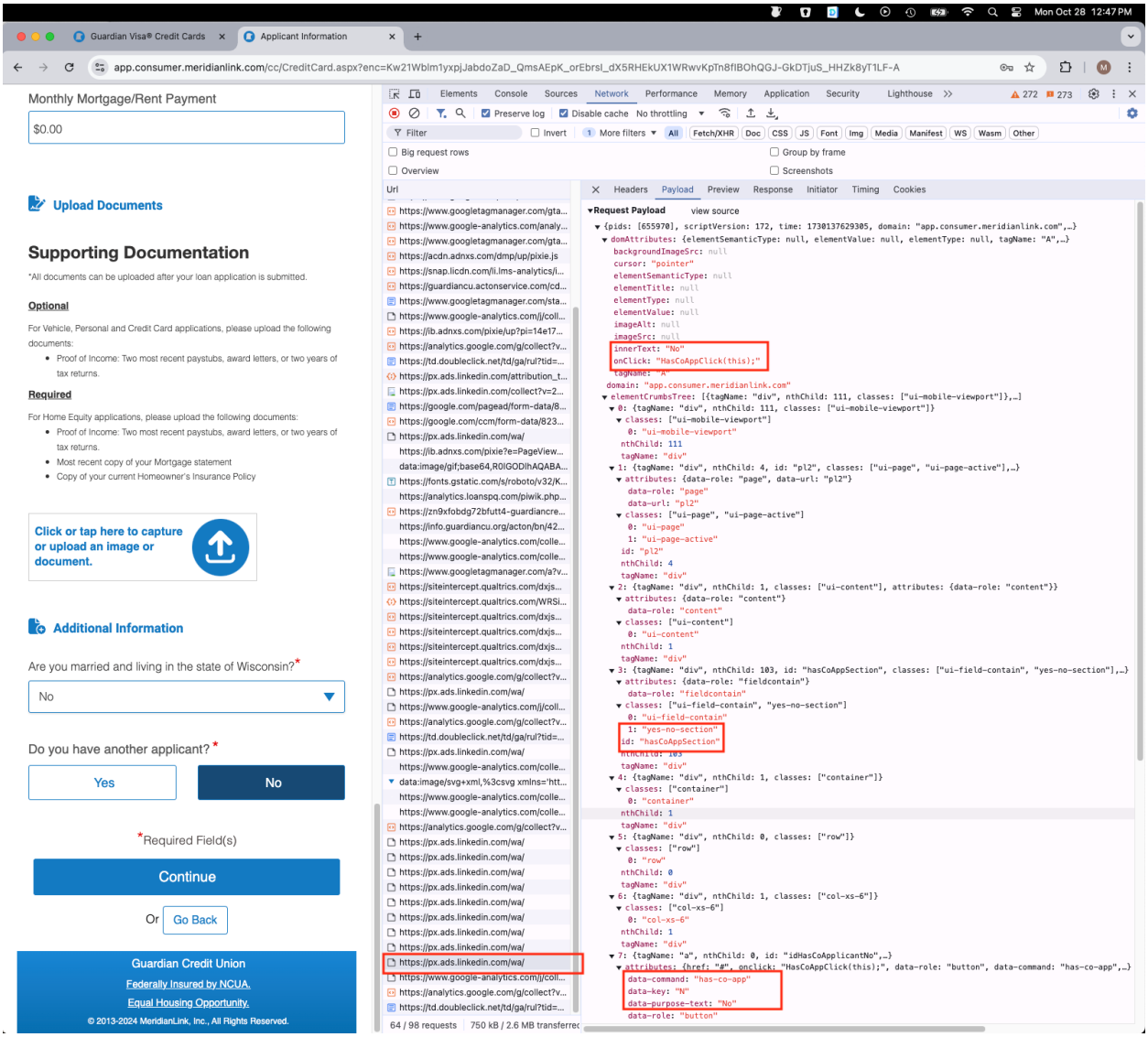


75. As users progress through the form, Guardian reports additional details from users' applications to LinkedIn, including the type of credit cards that users choose, whether they have co-applicants, and whether they agree to Guardian's disclosures.

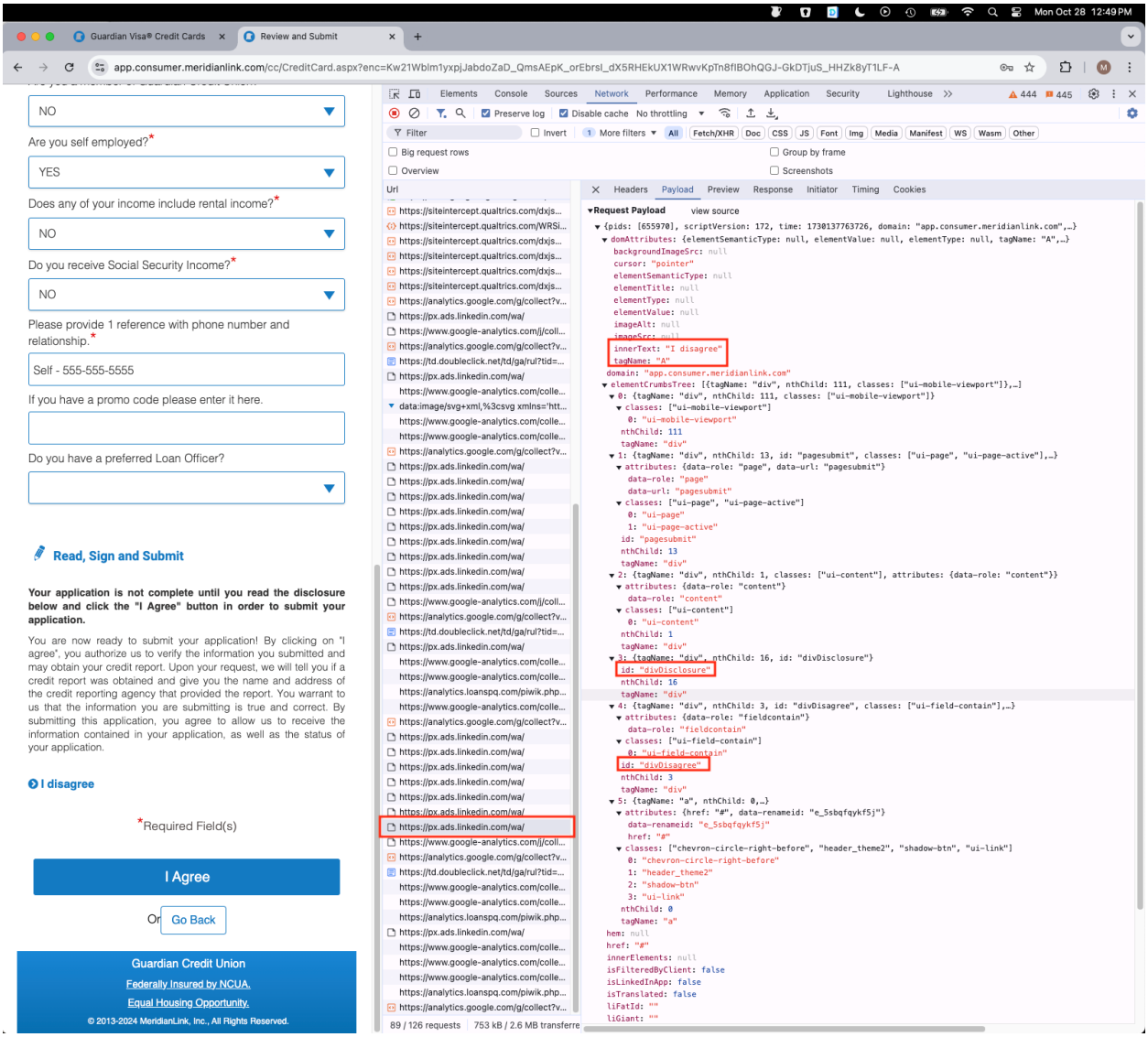
76. Users who apply for a new card are required by Guardian to choose the type of credit card that they would like. When a user selects their desired credit card, Guardian reports the user's selection to LinkedIn. For example, if a user applies for a Visa Platinum Rewards card, Guardian would send an event to LinkedIn disclosing that the user selected "Visa_Platinum_Rewards," from the "cc-options."



77. Additionally, when users indicate whether they have co-applicants for their credit card application, Guardian reports users' answers to LinkedIn. For instance, if a user who does not have a co-applicant were applying for a credit card, Guardian would send an event to LinkedIn disclosing that Guardian tagged the user with "idHasCoApplicantNo."



78. After users complete their credit card applications, Guardian prompts them to review their application and agree to a set of disclosures before submitting the application. If a user disagrees with the disclosures, Guardian reports this to LinkedIn, provided that the user selected "I disagree."



D. Guardian Maintains Ambiguous, Disingenuous, and Deceptive Privacy Policies That Fail to Sufficiently Disclose, Notify, Or Provide Opportunity to Opt-Out of the Disclosure

79. Customers never consented, agreed, authorized, or otherwise permitted Defendant to intercept their Personal and Financial Information or to use or disclose it for marketing and profit purposes. Customers were never provided with any written notice that Defendant disclosed their Personal and Financial Information to Third Parties (who then allowed fourth parties to use it for profit), nor were they provided means of opting out of such disclosures.

80. Customers relied on Defendant to keep their Personal and Financial Information confidential and securely maintained and to use this information only for the purpose of providing legitimate financial services. Customers relied on Defendant to make only authorized disclosures of this information.

81. Furthermore, Defendant actively misrepresented it would preserve the security and privacy of Customers' Personal and Financial Information.

82. The contracts that Guardian has with its Customers include Guardian's "Privacy Policy" which describes its "Online privacy policy,"[31] and "Full Privacy Policy"[32] on its Website (collectively, "Privacy Policies").

83. In its Privacy Policy, Guardian represents that it "respects your right to privacy," "[s]afeguard[s] members' and site users' information from unauthorized access, and [m]aintain[s] the confidentiality of member information which you provide to us."[33] But Guardian fails to "respect" Customers' privacy and private information, 'safeguard' Customers' information, or

[31] *Privacy Policy* (Exhibit A).

[32] *Full Privacy Policy*, https://www.guardiancu.org/wp-content/uploads/2019/10/PrivacyPolicy_0919.pdf (last visited Jan. 23, 2025) ("*Full Privacy Policy*" (Exhibit B).

[33] *Privacy Policy.*

"[m]aintain the confidentiality of member information," instead disclosing it to Third Parties (and eventually fourth parties) uninvolved in providing financial services to Plaintiff and Class Members and without Customers' authorization or consent.

84. Guardian explains that "[f]ederal law gives consumers the right to limit . . . sharing."[34] Guardian's Privacy Policy represents:

> Federal law also requires us to tell you how we collect, share, and protect your personal information . . . The types of personal information we collect and share depend on the product or service you have with us. . . . . This information can include:
>
> - Social Security number and account balances
> - Account transactions and credit card and other debt transactions
> - Payment history and transaction history[35]

85. But the types of personal information that Guardian collects and shares does ***not*** depend on the product or service a Customer has with it. Instead, Guardian indiscriminately collects and shares Customer information without regard to the product or service a Customer has with Guardian.

86. Guardian lists the "[r]easons we can share your personal information" which includes whether Guardian shares, "reasons" Guardian chooses to share, and whether Customers can "limit this sharing."[36] Those reasons include "our everyday business purposes-such as to process your transactions, maintain your accounts(s), respond to court orders and legal investigations, or report to credit bureaus"; "For our marketing purposes – to offer our products and services to you"; "For joint marketing with other financial companies"; "For our affiliates' everyday business purposes – information about your transactions and experiences"; "For our

[34] *Full Privacy Policy.*
[35] *Id.*
[36] *Id.*

affiliates' everyday business purposes – information about your creditworthiness"; "For our affiliates to market to you"; and "For our nonaffiliates to market to you."[37]

87. Guardian defines an Affiliate as "Companies related by common ownership or control. They can be financial and nonfinancial companies."[38] Third Parties like Google, which do not have a Guardian name, are not Guardian's affiliates.

88. Joint marketing is "A formal agreement between nonaffiliated financial companies that together market financial products or services to [Customers]."[39] Guardian's "joint marketing partners include insurance companies, credit card companies, and investment companies."[40] Certainly, Third Parties like Google do not meet this definition.

89. Guardian finally defines "nonaffiliates," which are "[c]ompanies not related by common ownership or control."[41] "They can be financial and nonfinancial companies."[42] Guardian represents that Customers can "limit this sharing."[43]

90. "Guardian Credit Union would like to assure [Customers] that [it] do[es] not: Collect personal information from you unless you provide it to us, or Sell the names and addresses of our members and site users to outside parties."[44]

91. With respect to its online policies, Guardian represents that it collects only "anonymous statistics to monitor our site's performance and inform our marketing efforts."[45] "We may use non-personally identifiable information such as cookies and IP addresses to provide

[37] *Id.*
[38] *Id.*
[39] *Id.*
[40] *Id.*
[41] *Id.*
[42] *Id.*
[43] *Id.*
[44] *Privacy Policy*.
[45] *Id.*

targeted marketing[;] While we gather this information, none of it is associated with you as an individual."[46]

92. Guardian further represents:

> you may be asked to give us personal information in order to apply for membership, a loan, or other services. Our application forms securely collect personal and financial information. The information that we collect on our applications is used only to process your request quickly and accurately.[47]

93. Customers reasonably understand that Guardian will securely maintain the Personal and Financial Information they entrusted to it and protect that information from being shared or utilized by Third Parties (and fourth parties) that have nothing to do with Guardian or its services. Guardian's Privacy Policies only reinforced this reasonable understanding.

94. Nowhere in the policies does Guardian disclose its use of Customer Personal and Financial Information for Third Party and fourth party marketing.

95. While Guardian offers Customers a Mail-in Form to "limit" Guardian's sharing of Customers' information,[48] the form in no way limits the way Guardian shares information through trackers.

96. Guardian's failure to safeguard the privacy of Customers' Personal and Financial Information as agreed in its Privacy Policies is even more egregious here, as Guardian also fails to provide Customers with sufficient opportunity to opt out of disclosure to nonaffiliates (or any other party, for that matter). This is because, as described above, while the Privacy Policies state that Customers may "limit this sharing," as described above, the Third Party trackers will still instantaneously send data from Customers that visit Guardian's Website even if a Customer calls

[46] *Id.*
[47] *Id.*
[48] *Id.*

the provided number or "go[es] to guardiancu.org"[49] and specifically requests that Guardian stop or otherwise limit the sharing of their Personal and Financial Information (i.e., after the Customer has 'opted out'). The trackers are active on Guardian's Website indiscriminately, regardless of what an individual Customer requests. Any opt-out request a Customer makes is thus entirely ineffective against Third Party trackers.

E. Guardian Violated the GLBA, FTC Standards, and Related Regulations

97. As a financial institution, Guardian is subject to the GLBA. 15 U.S.C. § 6809(3)(A) (a "financial institution" is "any institution the business of which is engaging in financial activities...").

98. Pursuant to the GLBA, "each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information." 15 U.S.C. § 6801(a).

99. The FTC has interpreted Section 5 of the FTC Act, 15 U.S.C. § 45, to include compliance with the GLBA Privacy Rule, 16 C.F.R. § 313.1 *et seq*. The FTC consistently enforces the GLBA Privacy Rule, as failure to comply with the GLBA Privacy Rule is an unfair act or practice prohibited by Section 5 of the FTC Act.[50]

100. The GLBA Privacy Rule is a regulation that "governs the treatment of nonpublic personal information about consumers by the financial institutions." 16 C.F.R. § 313.1 *et seq*.

101. Pursuant to the GLBA Privacy Rule, "[a] financial institution must provide a notice of its privacy policies and practices with respect to both affiliated and nonaffiliated third parties,

[49] *Privacy Policy* (Exhibit A).

[50] *See How to Comply with the Privacy Rule*, https://www.ftc.gov/business-guidance/resources/how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act (last visited Aug. 22, 2024) ("The FTC may bring enforcement actions for violations of the Privacy Rule.").

and allow the consumer to opt out of the disclosure of the consumer's nonpublic personal information to a nonaffiliated third party if the disclosure is outside of the exceptions."[51] Guardian consistently fails to do this.

102. The GLBA Privacy Rule, defines sensitive information that should not be indiscriminately disclosed:

> (n) (1) Nonpublic personal information means:
>
> (i) Personally identifiable financial information; and
>
> (ii) Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available.…
>
> (3) Examples of lists—
>
> (i) Nonpublic personal information includes any list of individuals' names and street addresses that is derived in whole or in part using personally identifiable financial information (that is not publicly available), such as account numbers.…
>
> (o) (1) Personally identifiable financial information means any information:
>
> (i) A consumer provides to you to obtain a financial product or service from you;
>
> (ii) About a consumer resulting from any transaction involving a financial product or service between you and a consumer; or
>
> (iii) You otherwise obtain about a consumer in connection with providing a financial product or service to that consumer.
>
> (2) Examples—
>
> (i) Information included. Personally identifiable financial information:
>
> (A) Information a consumer provides to you on an application to obtain a loan, credit card, or other financial product or service;
>
> (B) Account balance information, payment history, overdraft history, and credit or debit card purchase information;
>
> (C) The fact that an individual is or has been one of your customers or has obtained a financial product or service from you;
>
> (D) Any information about your consumer if it is disclosed in a manner that indicates that the individual is or has been your consumer;

[51] *See* FTC, *Financial Privacy Rule*, https://www.ftc.gov/legal-library/browse/rules/financial-privacy-rule (last visited August 8, 2024).

> (E) Any information that a consumer provides to you or that you or your agent otherwise obtain in connection with collecting on, or servicing, a credit account;
> (F) Any information you collect through an Internet "cookie" (an information collecting device from a web server); and
> (G) Information from a consumer report.

16 C.F.R. § 313.3

103. The information that Guardian disclosed to Third Parties via trackers—including *e.g.*, information when users apply or register for (i) a Guardian membership, (ii) banking portal, and (iii) credit cards, informing third parties about users' progression through the applications, and specific details including personally identifiable information that users provide to Guardian as part of the application processes—is "nonpublic personal information" under the GLBA and related regulations. 16 C.F.R. § 313.3.

104. Guardian has utterly failed to meet its privacy obligations under the GLBA: it has explicitly disclosed Customers' nonpublic personal information and Personal and Financial Information to Third Parties for marketing and advertisement, including for Third Party and fourth party advertising use, and refused to allow customers to meaningfully limit this sharing.

105. Guardian fails to meet its notice obligations under the GLBA. "[A] financial institution may not, directly or through any affiliate, disclose to a nonaffiliated third party any nonpublic personal information, unless such financial institution provides or has provided to the consumer a notice that complies with section 6803 of this title." 15 U.S.C.A. § 6802. As outlined at length above, Guardian's Privacy Policies fail to put Customers on notice as required here and actually promise that Customers' Personal and Financial Information will not be shared with Third Parties (and fourth parties) for targeted advertising purposes.

106. For example, by stating in its Privacy Policies that Guardian maintains the confidentiality of Customers' Personal and Financial Information and **does not** inform Customers that it sells their Personal and Financial Information to Third Parties for their use in their own advertising and marketing, the Privacy Policies fail to properly disclose:

> (1) the policies and practices of the institution with respect to disclosing nonpublic personal information to nonaffiliated third parties . . . including []the categories of persons to whom the information is or may be disclosed, other than the persons to whom the information may be provided [and] the policies and practices of the institution with respect to disclosing of nonpublic personal information of persons who have ceased to be customers of the financial institution . . .
>
> (2) the categories of nonpublic personal information that are collected by the financial institution; [and]
>
> (3) the policies that the institution maintains to protect the confidentiality and security of nonpublic personal information

15. U.S.C.A. § 6803.

107. As detailed above, Guardian also fails to meet its opt out obligations under the GLBA. The GLBA Privacy Rule requires financial institutions to, for example, "provide an opt out notice" to Customers, which notice "must state…[t]hat the consumer has the right to opt out of that disclosure [and] [a] reasonable means by which the consumer may exercise the opt out right." 16 C.F.R. § 313.7. Under the GLBA, Guardian

> may not disclose nonpublic personal information to a nonaffiliated third party unless—
>
> (A) [it] clearly and conspicuously discloses to the consumer. . . that such information may be disclosed to such third party;
>
> (B) ***the consumer is given the opportunity***, before the time that such information is initially disclosed, ***to direct that such information not be disclosed to such third party***; and
>
> (C) the consumer is given an explanation of how the consumer can exercise that nondisclosure option.

15 U.S.C.A. § 6802 (emphasis added).

108. Guardian fails to meet its opt out obligations because Customers are not provided an opportunity before disclosure to direct the nondisclosure of their information—as described above, Guardian instantaneously discloses information when Customers visit its Website.

109. Guardian further fails to meet its opt out obligations because it does not provide Customers with an explanation of how they can exercise a nondisclosure option.

110. Guardian still further fails to meet its opt out obligations because it fails to provide Customers with reasonable means of opting out. The GLBA Privacy Rule provides "examples of reasonable opportunity to opt out":

> (i) By mail. You mail the notices required in paragraph (a)(1) of this section to the consumer and allow the consumer to opt out by mailing a form, calling a toll-free telephone number, or any other reasonable means within 30 days from the date you mailed the notices.
> (ii) By electronic means. A customer opens an on-line account with you and agrees to receive the notices required in paragraph (a)(1) of this section electronically, and you allow the customer to opt out by any reasonable means within 30 days after the date that the customer acknowledges receipt of the notices in conjunction with opening the account.
> (iii) Isolated transaction with consumer. For an isolated transaction, such as the purchase of a money order by a consumer, you provide the consumer with a reasonable opportunity to opt out if you provide the notices required in paragraph (a)(1) of this section at the time of the transaction and request that the consumer decide, as a necessary part of the transaction, whether to opt out before completing the transaction.

16 C.F.R. § 313.10.

111. Guardian's only opt out procedure provides Customers with no real way to "opt-out"; and were a Customer to attempt to opt out, Guardian fails to comply with its opt out obligations because it fails to fully abide by its Customers' opt out. Calling the number or visiting Guardian's website does not actually opt a Customer out of sharing their information. This is not a "reasonable" means of opting out as outlined in the GLBA Privacy Rule. And anyway, Third

Party trackers will continue to instantaneously send data from Customers visiting Guardian's Website. Customers have **no** option to fully opt out of Disclosures to Third Parties or targeted advertising. This both fails to provide Customers with actual opportunity to opt out, and fails to abide by the opt out request, since Third Party trackers will continue to instantaneously send data from Customers visiting Guardian's Website. Customers have **no** option to fully opt out.

112. By perpetually disclosing its customers' Personal and Financial Information to third parties without consent, Guardian failed and continues to fail to meet its obligations under the GLBA, FTC standards, and related regulations, to establish appropriate standards and safeguards relative to Customers' Personal and Financial Information.

F. Plaintiff's Experiences

113. Plaintiff David Gassman has a Guardian debit card, has an online banking portal login, and has used Guardian's website for the last three years.

114. Plaintiff has used Defendant's Website to facilitate his financial services with Defendant and inputted Personal and Financial Information into Defendant's Website at Defendant's direction and encouragement.

115. Plaintiff is a Facebook user.

116. Plaintiff further applied for Defendant's services sometime in 2022, when he applied for a Guardian credit card. Guardian denied his application.

117. Shortly after Plaintiff used Defendant's Website to apply for a Guardian credit card, he received advertising on Facebook for different banks and applying for cards.

118. At no point did Customers like Plaintiff sign any written authorization permitting Defendant to send their Personal and Financial Information to Third Parties (or fourth parties) uninvolved in providing them with Defendant's financial services.

119. Plaintiff reasonably expected that his communications with Guardian were confidential, solely between each Plaintiff and Guardian, and that, as such, those communications and any Personal and Financial Information submitted would not be transmitted to or intercepted by a third party (or used by a fourth party).

120. Plaintiff provided his Personal and Financial Information to Defendant and trusted that the information would be safeguarded according to Guardian's promises and the law.

121. Plaintiff never intended to sell his Personal and Financial Information, nor would he have permitted it to be made available for sale on the resale market.

122. Plaintiff never intended to let Guardian benefit from his Personal and Financial Information.

123. Through the systematic data sharing process described in this complaint, Plaintiff's interactions with Guardian's Website were disclosed to Third Parties, including Facebook and Google. Plaintiff did not consent to those disclosures.

124. On information and belief, through its use of Third Party trackers on its Website, Defendant disclosed to Third Parties information Plaintiff provided to Guardian as a financial institution and resulting from a transaction for Plaintiff to obtain Defendant's credit card, including each Plaintiff's:

a. Credit card application information;

b. Existing membership, or Customer, status;

c. Purpose for applying for a credit card;

d. The specific credit card Plaintiff applied for;

e. Whether Plaintiff agreed with the disclosures; and

f. Co-applicant information.

125. By failing to receive the requisite consent, Guardian breached confidentiality and unlawfully disclosed Plaintiff's Personal and Financial Information.

126. Plaintiff would not have submitted his information to Guardian if he had known it would be shared with Third Parties and fourth parties.

127. As a result of Guardian's Disclosure of Plaintiff's Personal and Financial Information via the Google trackers and other tracking technologies to Third Parties (and fourth parties) without authorization, Plaintiff suffered the following injuries:

a. Loss of privacy; unauthorized disclosure of his Personal and Financial Information; unauthorized access of his Personal and Financial Information by Third Parties;

b. Guardian benefited from the use of Plaintiff's Personal and Financial Information without sharing that benefit with Plaintiff;

c. Plaintiff now receives targeted advertisements from Third and Fourth Parties on social media, reflecting his Personal and Financial Information that was improperly disclosed and used;

d. Plaintiff paid Guardian for financial services, and the services he paid for included reasonable privacy and data security protections for his Personal and Financial Information, but due to Defendant's Disclosure, Plaintiff did not receive the privacy and security protections for which he paid;

e. The portion of Guardian's revenues and profits attributable to collecting Plaintiff's Personal and Financial Information without authorization and sharing it with Third Parties (and fourth parties);

f. The portion of Guardian's savings in marketing costs attributable to collecting Plaintiff's Personal and Financial Information without authorization and sharing it with Third Parties (and fourth parties);

g. The portion of Guardian's revenues and profits attributable to serving and monetizing advertisements directed to Plaintiff as a result of collecting Plaintiff's Personal and Financial Information without authorization and sharing it with Third Parties (and fourth parties);

h. Value to Plaintiff of surrendering his choice to keep his Personal and Financial Information private and allowing Guardian to track his data;

i. Embarrassment, humiliation, frustration, and emotional distress;

j. Decreased value of Plaintiff's Personal and Financial Information;

k. Lost benefit of the bargain;

l. Increased risk of future harm resulting from future use and disclosure of his Personal and Financial Information; and

m. Statutory damages.

TOLLING, CONCEALMENT, AND ESTOPPEL

128. The applicable statutes of limitation have been tolled as a result of Guardian's knowing and active concealment and denial of the facts alleged herein.

129. Guardian seamlessly incorporated trackers into its Website while providing Customers using those platforms with no indication that its Website usage was being tracked and transmitted to Third Parties. Guardian knew that its Website incorporated trackers, yet it failed to disclose to Plaintiff and Class Members that their sensitive Personal and Financial Information would be intercepted, collected, used by, and disclosed to Third Parties.

130. Plaintiff and Class Members could not with due diligence have discovered the full scope of Guardian's conduct, because there were no disclosures or other indication that they were interacting with websites employing tracking technology to unauthorizedly disclose their Personal and Financial Information.

131. All applicable statutes of limitation have also been tolled by operation of the discovery rule and the doctrine of continuing tort. Guardian's illegal interception and disclosure of Plaintiff's and the Class's Personal and Financial Information has continued unabated. What is more, Guardian was under a duty to disclose the nature and significance of its data collection practices but did not do so. Guardian is therefore estopped from relying on any statute of limitations defenses.

CLASS ACTION ALLEGATIONS

132. Plaintiff brings this nationwide class action on behalf of himself and on behalf of all other similarly situated persons pursuant to Fed. R. Civ. P. 23.

133. Plaintiff seeks to represent the following classes:

> **Nationwide Class**: All individuals in the United States whose Personal and Financial Information was disclosed by Defendant to Third Parties through Defendant's Website's tracking technology without authorization.
>
> **Wisconsin Subclass**: All individuals in Wisconsin whose Personal and Financial Information was disclosed by Defendant to Third Parties through Defendant's Website's tracking technology without authorization.

134. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers, and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

135. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

136. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23(a)(1)-(4).

137. Numerosity: Class Members are so numerous and geographically dispersed that joinder of all members is impracticable. Upon information and belief, there likely thousands of individuals throughout the United States whose Personal and Financial Information has been improperly used or disclosed by Defendant, and the Classes are identifiable within Defendant's records.

138. Ascertainability. Class Members are readily identifiable from information in Defendant's possession, custody, and control.

139. Commonality and Predominance: Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether Defendant disclosed Class Members' Personal and Financial Information to Third Parties;

b. Whether Class Members consented to Defendant's disclosure of their Personal and Financial Information;

c. Whether Defendant owed duties to Plaintiff and Class Members to protect their Personal and Financial Information;

d. Whether Defendant breached its duty to protect Plaintiff's and Class Members' Personal and Financial Information;

e. Whether Defendant's disclosure of Plaintiff's and Class Members' Personal and Financial Information to Third Parties violated federal, state and local laws, or industry standards;

f. Whether Defendant's failure to allow Customers a meaningful opportunity to opt out of sharing with Third Parties violated federal, state and local laws, or industry standards;

g. Whether Defendant's conduct resulted in or was the actual cause of the disclosure of Plaintiff's and Class Members' and Personal and Financial Information;

h. Whether Defendant's conduct resulted in or was the proximate cause of the disclosure of Plaintiff's and Class Members' Personal and Financial Information;

i. Whether Defendant has a contractual obligation to protect Plaintiff's and Class Members' Personal and Financial Information and whether it complied with such contractual obligation;

j. Whether Defendant has a duty sounding in bailment to protect Plaintiff's and Class Members' Personal and Financial Information and whether it complied with such obligation;

k. Whether Defendant has a duty of confidence and whether it complied with such obligation;

l. Whether Defendant's conduct amounted to violations of state consumer protection statutes;

m. Whether Defendant's conduct amounted to violations of state and federal wiretap statutes;

n. Whether Defendant's conduct amounted to violations of other Wisconsin state laws;

o. Whether Defendant should retain Plaintiff's and Class Members' valuable Personal and Financial Information; and

p. Whether, as a result of Defendant's conduct, Plaintiff and Class Members are entitled to injunctive, equitable, declaratory and/or other relief, and, if so, the nature of such relief.

140. Defendant has engaged in a common course of conduct toward Plaintiff and the Class Members, in that the Plaintiff's and Class Members' data was stored on the same computer system and unlawfully disclosed and accessed in the same way. As set forth above, the common issues arising from Defendant's conduct affecting Class Members predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

141. Typicality: Plaintiff's claims are typical of those of other Class Members because all had their Personal and Financial Information compromised as a result of Defendant's use and incorporation of Google trackers and other tracking technology.

142. Policies Generally Applicable to the Classes: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Classes as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly, and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Classes as a whole, not on facts or law applicable only to Plaintiff.

143. Adequacy: Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic

to those of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages Plaintiff has suffered is typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

144. Superiority and Manageability: Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

145. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged. If the class action device were not used, Defendant would necessarily gain an unconscionable advantage because it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources. Moreover, the costs of individual suits could unreasonably consume the amounts that would be recovered, whereas proof of a common course of conduct to which Plaintiff were exposed is representative of that experienced by the Classes and will establish the right of each Class Member to recover on the cause of action alleged. Finally, individual actions

would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

146. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

147. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

148. Unless a Class-wide injunction is issued, Defendant may continue in its unlawful use and disclosure and failure to properly secure the Personal and Financial Information of Plaintiff and the Class Members, Defendant may continue to refuse to provide proper notification to and obtain proper consent from Class Member, and Defendant may continue to act unlawfully as set forth in this Complaint.

149. Moreover, Defendant has acted or refused to act on grounds generally applicable to the Classes, and, accordingly, final injunctive or corresponding declaratory relief regarding the whole of the Classes is appropriate.

150. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to the following:

a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Personal and Financial Information;

b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Personal and Financial Information;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to the disclosure of customer information;

d. Whether Defendant was negligent and/or negligent *per se*;

e. Whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that contract;

f. Whether Defendant breached the contract;

g. In the alternate, whether Defendant was unjustly enriched;

h. Whether a bailment existed between Defendant on the one hand, and Plaintiff and Class Members on the other;

i. Whether Defendant breached its bailment duty;

j. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their Personal and Financial Information had been used and disclosed to Third Parties and used for Third Party and fourth party benefit;

k. Whether Defendant adequately provided opt-out measures;

l. Whether Defendant abided by Plaintiff's and Class Members' opt-out requests;

m. Whether Defendant failed to implement and maintain reasonable security procedures and practices;

n. Whether Defendant invaded Plaintiff and the Class Members' privacy;

o. Whether Defendant breached its implied duty of confidentiality; and,

p. Whether Plaintiff and the Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Classes)

151. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

152. Plaintiff and Class Members submitted sensitive nonpublic personal information, including Personal and Financial Information, when accessing Guardian's Website.

153. Defendant owed to Plaintiff and Class Members a duty to exercise reasonable care in handling and using Plaintiff's and Class Members' Personal and Financial Information in its care and custody, including implementing industry-standard privacy procedures sufficient to reasonably protect the information from the disclosure and unauthorized transmittal and use of Personal and Financial Information that occurred.

154. Defendant's duties to keep the nonpublic personal information, including Personal and Financial Information, confidential also arose under the GLBA, which imposes "an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information." 15 U.S.C. § 6801(a).

155. Defendant's duties to keep the nonpublic personal information, including Personal and Financial Information, confidential also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including the unfair practice of failing to keep the nonpublic personal information confidential.

156. Defendant acted with wanton and reckless disregard for the privacy and confidentiality of Plaintiff's and Class Members' Personal and Financial Information by disclosing

and providing access to this information to the Third Parties for the financial benefit of the Third Parties (and fourth parties) and Defendant.

157. Defendant owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's disclosure of their Personal and Financial Information to benefit Third Parties (and fourth parties) and Defendant. Defendant actively sought and obtained Plaintiff's and Class Members' Personal and Financial Information. And Defendant knew or should have known that by integrating tracking technology on its Website that Plaintiff's and Class Members' nonpublic personal information, including Personal and Financial Information, would be disclosed to the Third Parties (and used by the fourth parties).

158. Personal and Financial Information is highly valuable, and Defendant knew, or should have known, the harm that would be inflicted on Plaintiff and Class Members by disclosing their Personal and Financial Information to the Third Parties. This disclosure was of benefit to the Third Parties (and fourth parties) and Defendant by way of data harvesting, advertising, and increased sales.

159. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers in the handling and securing of Personal and Financial Information of Plaintiff and Class Members. This failure actually and proximately caused Plaintiff's and Class Members' injuries.

160. As a direct, proximate, and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and Class Members have suffered or imminently will suffer injury and damages, including monetary damages, inappropriate advertisements and use of their Personal

and Financial Information for advertising purposes, and increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

161. Defendant's breach of its common-law duties to exercise reasonable care and negligence, directly and proximately caused Plaintiff's and Class Members' actual, tangible, injury-in-fact and damages, including, without limitation: the unauthorized access of their Personal and Financial Information by Third Parties (and fourth parties); improper disclosure of their Personal and Financial Information; receipt of targeted advertisements reflecting private financial information; lost benefit of their bargain; lost value of their Personal and Financial Information and diminution in value; embarrassment, humiliation, frustration, and emotional distress; lost time and money incurred to mitigate and remediate the effects of use of their information, as to targeted advertisements that resulted from and were caused by Defendant's negligence; value to Plaintiff and the Class Members of surrendering their choices to keep their Personal and Financial Information private and allowing Defendant to track their data; increased risk of future harm resulting from future use and disclosure of Plaintiff's and the Class Members' Personal and Financial Information; and other injuries and damages as set forth herein. These injuries are ongoing, imminent, immediate, and continuing.

162. Defendant's negligence directly and proximately caused the unauthorized access and Disclosure of Plaintiff's and Class Members' Personal and Financial Information, and as a result, Plaintiff and Class Members have suffered and will continue to suffer damages as a result of Defendant's conduct. Plaintiff and Class Members seek actual and compensatory damages, and all other relief they may be entitled to as a proximate result of Defendant's negligence.

163. Plaintiff and Class Members seek to recover the value of the unauthorized access to their Personal and Financial Information resulting from Defendant's wrongful conduct. This

measure of damages is analogous to the remedies for unauthorized use of intellectual property. Like a technology covered by a trade secret or patent, use or access to a person's personal information is non-rivalrous—the unauthorized use by another does not diminish the rights-holder's ability to practice the patented invention or use the trade-secret protected technology. Nevertheless, a Plaintiff may generally recover the reasonable use value of the intellectual property—i.e., a "reasonable royalty" from an infringer. This is true even though the infringer's use did not interfere with the owner's own use (as in the case of a non-practicing patentee) and even though the owner would not have otherwise licensed such intellectual property to the infringer. A similar royalty or license measure of damages is appropriate here under common law damages principles authorizing recovery of rental or use value. This measure is appropriate because (a) Plaintiff and Class Members have a protectible property interest in their Personal and Financial Information; (b) the minimum damages measure for the unauthorized use of personal property is its rental value; and (c) rental value is established with reference to market value, i.e., evidence regarding the value of similar transactions

164. Plaintiff and Class Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Defendant's actions, directed at injuring Plaintiff and Class Members in conscious disregard of their rights. Such damages are needed to deter Defendant from engaging in such conduct in the future.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Classes)

165. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

166. Plaintiff brings this negligence *per se* count in the alternative to the common law negligence claim.

167. Pursuant to the laws set forth herein, including the FTC Act, the GLBA, and state law, Defendant was required by law and industry standards to maintain adequate and reasonable data and cybersecurity measures to maintain the security and privacy of Plaintiff's and Class Members' Personal and Financial Information.

168. Plaintiff and Class Members are within the class of persons that these statutes and rules were designed to protect.

169. Defendant had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' Personal and Financial Information.

170. Defendant owed a duty to timely and adequately inform Plaintiff and Class Members, in the event of their Personal and Financial Information being improperly disclosed to unauthorized Third Parties.

171. It was not only reasonably foreseeable, but it was intended, that the failure to reasonably protect and secure Plaintiff's and Class Members' Personal and Financial Information in compliance with applicable laws would result in unauthorized Third Parties and fourth parties gaining access to Plaintiff's and Class Members' Personal and Financial Information, and resulting in Defendant's liability under principles of negligence *per se*.

172. Defendant violated its duty under Section 5 of the FTC Act, the GLBA, and/or state law by failing to use reasonable measures to protect Plaintiff's and Class Members' Personal and Financial Information and not complying with applicable industry standards as described in detail herein.

173. Plaintiff's and Class Member's Personal and Financial Information constitutes personal property that was taken and misused as a proximate result of Defendant's negligence, resulting in harm, injury and damages to Plaintiff and Class Members.

174. As a proximate result of Defendant's negligence *per se* and breach of duties as set forth above, Plaintiff and Class Members were caused to, *inter alia*, have their data shared with Third Parties and fourth parties without their authorization or consent, receive unwanted advertisements that reveal seeking financial advice for specific issues, fear, anxiety and worry about the status of their Personal and Financial Information, diminution in the value of their personal data for which there is a tangible value, and/or a loss of control over their Personal and Financial Information, all of which can constitute actionable actual damages.

175. Defendant's conduct in violation of applicable laws directly and proximately caused the unauthorized access and disclosure of Plaintiff's and Class Members' Personal and Financial Information, and as a result, Plaintiff and Class Members have suffered and will continue to suffer damages as a result of Defendant's conduct. Plaintiff and Class Members seek actual, and compensatory damages, and all other relief they may be entitled to as a proximate result of Defendant's negligence *per se*.

176. Plaintiff and Class Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Defendant's actions, directed at injuring Plaintiff and Class Members in conscious disregard of their rights. Such damages are needed to deter Defendant from engaging in such conduct in the future.

COUNT III
INVASION OF PRIVACY—INTRUSION UPON SECLUSION
WIS. STAT. 995.50
(On Behalf of Plaintiff and the Classes)

177. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

178. Wisconsin recognizes the tort of invasion of privacy – intrusion upon seclusion.

179. In Wisconsin, the tort of invasion of privacy intrusion upon seclusion is defined as "[i]ntrusion upon the privacy of another of a nature highly offensive to a reasonable person…in a

place that a reasonable person would consider private, or in a manner that is actionable for trespass." Wis. Stat. Ann. § 995.50.

180. Plaintiff and Class Members had a reasonable expectation of privacy in their communications with Defendant via its Website.

181. Defendant's Website, a place where Customers like Plaintiff and Class Members communicated sensitive Personal and Financial Information, is a place that a reasonable person would consider private. While using Defendant's Website, Plaintiff and Class Members communicated sensitive Personal and Financial Information that they intended for only Defendant to receive and that they understood Defendant would keep private. Plaintiff's and Class Members' Personal and Financial Information is extremely private and not a matter of legitimate public interest.

182. As set forth above, Defendant disclosed Plaintiff's and the Class Members' Personal and Financial Information and confidential communications to Google and other third parties, without their authorization or knowledge.

183. Defendant's disclosure of the substance and nature of those communications to Third Parties without the knowledge and consent of Plaintiff and Class Members is an intentional intrusion on Plaintiff's and Class Members' solitude or seclusion in their private affairs and concerns.

184. Plaintiff and Class Members had a reasonable expectation of privacy in their communications over the Website. This expectation is further reinforced given their relationship with Defendant as a financial institution. Furthermore, Defendant's Privacy Policies enforced this reasonable expectation. Moreover, Plaintiff and Class Members have a general expectation that

their communications regarding Personal and Financial Information with their financial institution will be kept confidential.

185. Plaintiff and Class Members reasonably expected that their private communications with the Website would not be tracked, surveilled, recorded, eavesdropped, or otherwise intruded upon, and that their confidential communications with their financial institution would remain private.

186. Defendant intentionally intruded upon Plaintiff and Class Members' privacy by secretly recording their usage of the Website, including the Personal and Financial Information and confidential communications included therein.

187. Defendant's disclosure of Personal and Financial Information is highly offensive to the reasonable person.

188. As a result of Defendant's actions, Plaintiff and Class Members have suffered harm and injury, including but not limited to an invasion of their privacy rights, and other injuries and damages as set forth in the preceding paragraphs.

189. Plaintiff and Class Members have been damaged as a direct and proximate result of Defendant's invasion of their privacy and are entitled to just compensation, including monetary damages.

190. Plaintiff and Class Members seek appropriate relief for that injury, including but not limited to, damages that will reasonably compensate Plaintiff and Class Members for the harm to their privacy interests as a result of its intrusions upon Plaintiff's and Class Members' privacy.

191. Specifically, under Wisconsin's statutory right to privacy, Plaintiff is entitled to equitable relief, compensatory damages, and attorney fees. Wis. Stat. Ann. § 995.50.

192. Plaintiff and Class Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Defendant's actions, directed at injuring Plaintiff and Class Members in conscious disregard of their rights. Such damages are needed to deter Defendant from engaging in such conduct in the future.

193. Plaintiff also seeks such other relief as the Court may deem just and proper.

COUNT IV
INVASION OF PRIVACY – DISCLOSURE OF PRIVATE FACTS
WIS. STAT. 995.50
(On Behalf of Plaintiff and the Wisconsin Subclass)

194. Plaintiff re-alleges and incorporates the preceding paragraphs as if fully set forth herein.

195. Wisconsin also recognizes the tort of invasion of privacy – disclosure of private facts.

196. The tort of disclosure of private facts is defined as "[p]ublicity given to a matter concerning the private life of another, of a kind highly offensive to a reasonable person, if the defendant has acted either unreasonably or recklessly as to whether there was a legitimate public interest in the matter involved, or with actual knowledge that none existed." Wis. Stat. Ann. § 995.50.

197. Plaintiff and Class Members' Personal and Financial Information is extremely private and not a matter of legitimate public interest. Defendant knew this, and/or acted unreasonably or recklessly as to whether there was a legitimate public interest in its Customers' Personal and Financial Information.

198. The unauthorized disclosure of Personal and Financial Information by a financial institution, such as Defendant, is highly offensive to a reasonable person.

199. Defendant intentionally configured and installed tracking technologies on its Website, which it then used to record Plaintiff and Class Members' Personal and Financial Information and disclose that Personal and Financial Information to Third Parties.

200. By sharing Plaintiff and Class Members' Personal and Financial Information with Third Parties, Defendant gave publicity to the private lives of Plaintiff and Class Members.

201. Defendant acted with a knowing state of mind when it used source code tools specifically designed to track and record patients' Personal and Financial Information and disclose that Personal and Financial Information to third parties.

202. As a proximate result of Defendant's acts and omissions, Plaintiff's and Class Members' Personal and Financial Information was disclosed to Third Parties—and is now available for further disclosure and redisclosure without authorization, further inflicting injuries on Plaintiff and the Class.

203. As a result of Defendant's actions, Plaintiff and Class Members have suffered harm and injury, including but not limited to an invasion of their privacy rights.

204. Plaintiff and Class Members have been damaged as a direct and proximate result of Defendant's invasion of their privacy and are entitled to just compensation, including monetary damages.

205. Plaintiff and Class Members seek appropriate relief for that injury, including but not limited to, damages that will reasonably compensate Plaintiff and Class Members for the harm to their privacy interests as a result of Defendant's unlawful disclosure.

206. Specifically, under Wisconsin's statutory right to privacy, Plaintiff is entitled to equitable relief, compensatory damages, and attorney fees. Wis. Stat. Ann. § 995.50.

207. Plaintiff and Class Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Defendant's actions, directed at injuring Plaintiff and Class Members in conscious disregard of their rights. Such damages are needed to deter Defendant from engaging in such conduct in the future.

208. Plaintiff also seeks such other relief as the Court may deem just and proper.

COUNT V
CONVERSION
(On Behalf of Plaintiff and the Wisconsin Subclass)

209. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

210. Wisconsin recognizes the tort of conversion. In Wisconsin, conversion is "the wrongful exercise of dominion or control over a chattel." *Prod. Credit Ass'n of Chippewa Falls v. Equity Coop Livestock Sales Ass'n*, 82 Wis. 2d 5, 10 (1978).

211. Defendant committed criminal conversion as defined by W.S.A. 943.20.

212. Defendant committed tortious conversion by appropriating Plaintiff's and Class Members' personal property (i.e., the Personal and Financial Information) to Defendant's own use and benefit, as outlined above. Defendant disclosed Plaintiff's and Class Members Personal and Financial Information to Third Parties (and Fourth Parties) for profit and marketing purposes.

213. Defendant exerted unauthorized control over Plaintiff's and Class Members' personal property (i.e., the Personal and Financial Information) by sharing or disclosing Personal and Financial Information to Third Parties (and fourth parties).

214. Defendant knowingly and intentionally exerted unauthorized control over Plaintiff's and Class Members' Personal and Financial Information because Defendant knowingly and deliberately installed trackers that collected and disclosed Plaintiff's and Class Members' Personal and Financial Information to Third Parties (and Fourth Parties)

215. Plaintiff and Class Members received no benefit from Defendant's Disclosure.

216. Plaintiff and Class Members have suffered, and are suffering, pecuniary losses as a result of Defendant's conversion.

217. Plaintiff seeks all monetary and non-monetary relief allowed by law.

COUNT VI
TRESPASS TO CHATTEL
(On Behalf of Plaintiff and the Wisconsin Subclass)

218. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

219. Plaintiff brings this claim for trespass to chattel in the alternate to his other causes of action, or in addition to said claims, as allowed by law.

220. Wisconsin recognizes the tort of trespass to chattels. An intentional interference with the possession or physical condition of a chattel in the possession of another, without justification, is a trespass. *Wisconsin Power & Light Co. v. Columbia Cnty.*, 3 Wis. 2d 1, 8 (1958).

221. At all relevant times, Plaintiff and the Class Members had good and rightful ownership and possession of their Personal and Financial Information, which constitutes personal property.

222. By conduct alleged in the preceding paragraphs, Defendant intentionally exercised authority over and used the personal property of Plaintiff and the Class Members, their Personal and Financial Information, in an unauthorized manner, and intermeddled in this property, by sharing or disclosing this information to Third Parties (and Fourth Parties), including Google, without Plaintiff's and Class Members' authorization.

223. Further, Defendant obtained the Personal and Financial Information of Plaintiff and the Class Members through fraud or duress, by promising Plaintiff and the Class, in Defendant's Privacy Policies and elsewhere, that Defendant would preserve the confidentiality of this Personal

and Financial Information and not disclose it to Third Parties (or Fourth Parties) for marketing purposes without authorization.

224. Defendant knowingly and intentionally exerted unauthorized authority over and used Plaintiff's and Class Members' Personal and Financial Information, because Defendant knowingly and deliberately installed trackers on their Online Platforms that collected and disclosed Plaintiff's and Class Members' Personal and Financial Information to Third Parties (and Fourth Parties).

225. Defendant's trespass was a legal cause of injury-in-fact and damage to Plaintiff and the Class, including but not limited to loss of value of Plaintiff's and the Class's Personal and Financial Information, loss of use and beneficial enjoyment of the personal property, and other injuries and damages set forth herein.

226. As a direct and proximate result of Defendant's trespass to chattel, Plaintiff and Class Members are entitled to and do demand actual, consequential, and nominal damages, injunctive relief, and all other relief allowed by law.

COUNT VII
BREACH OF CONFIDENCE
(On Behalf of Plaintiff and the Classes)

227. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

228. At all times during Plaintiff's and Class Members' interactions with Guardian, Guardian was fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' Personal and Financial Information.

229. As alleged herein and above, Guardian's relationship with Plaintiff and Class Members was governed by terms and expectations that Plaintiff's and Class Members' Personal and Financial Information would be collected, stored, and protected in confidence, and would not

be disclosed to Third Parties, or used by Third Parties (and fourth parties) without Customers' notice and consent.

230. Plaintiff and Class Members provided Guardian with their Personal and Financial Information, with the explicit and implicit understandings that Guardian would protect and not permit that information to be disseminated to and used by unaffiliated Third Parties (and fourth parties) without notice, consent, and sufficient opportunity to opt out.

231. Guardian voluntarily received in confidence Plaintiff's and Class Members' Personal and Financial Information, with the understanding and affirmative representation to Customers that the information would not be disclosed or disseminated to unaffiliated Third Parties for Third Parties' (and fourth parties') marketing purposes.

232. Guardian disclosed Plaintiff's and Class Members' Personal and Financial Information, without notice, without express permission, and without opportunity to opt out.

233. But for Guardian's Disclosure of Plaintiff's and Class Members' Personal and Financial Information, in violation of the parties' understanding of confidence, their Personal and Financial Information would not have been disclosed to Third Parties, or used for Third Party (and fourth party) marketing and profit, without Customers' consent.

234. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Guardian's nonconsensual disclosure of Plaintiff's and Class Members' Personal and Financial Information. Guardian knew it was disclosing Plaintiff's and Class Members' Personal and Financial Information to Third Parties, for Third Party (and fourth party) use, without their consent.

235. As a direct and proximate result of Guardian's breaches of confidence, Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial.

236. Plaintiff seeks all monetary and non-monetary relief allowed by law.

COUNT VIII
BREACH OF EXPRESS AND IMPLIED CONTRACT
(On Behalf of Plaintiff and the Classes)

237. Plaintiff re-alleges and incorporates the preceding paragraphs as if fully set forth herein.

238. Plaintiff and Class Members also entered into an express and implied contract with Guardian when they obtained financial services from Guardian, or otherwise provided nonpublic personal information, including Personal and Financial Information, to Guardian.

239. As part of these transactions, Guardian explicitly and implicitly agreed to safeguard and protect Plaintiff's and Class Members' Personal and Financial Information.

240. Plaintiff and Class Members entered into express and implied contracts with the reasonable expectation (based on Guardian's own express and implied promises) that Guardian would keep their nonpublic personal information, including Personal and Financial Information, confidential. Plaintiff and Class Members believed that Guardian would use part of the monies paid to Guardian under the express and implied contracts to keep their nonpublic personal information, including Personal and Financial Information, confidential.

241. Plaintiff and Class Members would not have provided and entrusted their nonpublic personal information, including Personal and Financial Information, or would have paid less for Guardian's services in the absence of the express and implied contract or implied terms between them and Guardian. The safeguarding of the nonpublic personal information, including Personal and Financial Information, of Plaintiff and class members was critical to realize the intent of the parties.

242. As extensively detailed above, Guardian breached its express and implied contracts with Plaintiff and class members to protect their nonpublic personal information, including Personal and Financial Information, when it disclosed that information to Third Parties.

243. As a direct and proximate result of Guardian's breach of express and implied contract, Plaintiff and Class Members sustained actual losses and damages as described in detail above.

COUNT IX
UNJUST ENRICHMENT (IN THE ALTERNATIVE TO CONTRACT CLAIMS)
(On Behalf of Plaintiff and the Classes)

244. Plaintiff re-alleges and incorporates the preceding paragraphs as if fully set forth herein.

245. Plaintiff and Class Members have an equitable, legal, and financial interest in their Personal and Financial Information that was conferred upon, collected by, and maintained by Defendant and that was ultimately disclosed without their consent.

246. Plaintiff and Class Members conferred a monetary benefit upon Defendant in the form of valuable, sensitive, personal, and financial information—Personal and Financial Information—that Defendant collected from Plaintiff and Class Members under the guise of keeping this information private. Defendant collected, used, and disclosed this information for its own gain, for marketing purposes, and for sale or trade with Third Parties. Defendant did not share this benefit with Plaintiff and Class Members.

247. Plaintiff and Class Members would not have used Defendant's services, or would have paid less for those services, if they had known that Defendant would collect, use, and disclose their Personal and Financial Information to Third Parties or allow Third Parties (and fourth parties) to use their Personal and Financial Information.

248. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiff and Class Members.

249. The benefits that Defendant derived from Plaintiff and Class Members rightly belong to Plaintiff and Class Members themselves. Under unjust enrichment principles, it would be inequitable for Defendant to retain the profit and/or other benefits it derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

250. Defendant continues to benefit and profit from its retention and use of Plaintiff's and Class Members' Personal and Financial Information, while its value to Plaintiff and Class Members has been diminished.

251. Plaintiff pleads this claim separately as well as in the alternative to claims for damages under Fed. R. Civ. P. 8(a)(3), because if the Court dismisses Plaintiff's claims for damages or enters judgment on them in favor of the Defendant, Plaintiff's will have no adequate legal remedy. Plaintiff makes the following allegations in this paragraph only hypothetically and as an alternative to any contrary allegations in her other causes of action, in the event that such causes of action do not succeed. Plaintiff and the Class Members may be unable to obtain monetary, declaratory and/or injunctive relief directly under other causes of action, and, if so, will lack an adequate remedy at law.

252. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds it received as a result of the conduct and the unauthorized Disclosure alleged herein.

COUNT X
BAILMENT
(On Behalf of Plaintiff and the Classes)

253. Plaintiff re-alleges and incorporates the preceding paragraphs as if fully set forth herein.

254. Plaintiff, Class Members, and Defendant contemplated a mutual benefit bailment when Plaintiff and Class Members transmitted their Personal and Financial Information to Defendant solely for financial services and the payment thereof.

255. Plaintiff's and Class Members' Personal and Financial Information was transmitted to Defendant in trust for a specific and sole purpose of receiving Guardian's financial services, with an implied contract that the trust was to be faithfully executed, and the Personal and Financial Information was to be accounted for when the special purpose was accomplished.

256. Defendant was duty bound under the law to exercise ordinary care and diligence in safeguarding Plaintiff's and Class Members' Personal and Financial Information.

257. Plaintiff's and Class Members' Personal and Financial Information was used for a different purpose than Plaintiff and Class Members intended, for a longer time period and/or in a different manner or place than the parties intended.

258. Defendant's breach of the bailment was a legal cause of injury-in-fact and damage to Plaintiff and Class Members, including but not limited to, the unauthorized access of their Personal and Financial Information by Third Parties, improper use of their Personal and Financial Information by Third Parties and fourth parties, improper disclosure of their Personal and Financial Information, lost benefit of their bargain, lost value of their Personal and Financial Information, and lost time and money incurred to mitigate and remediate the effects of use of their information that resulted from and were caused by Defendant's tortious conduct. These injuries are ongoing, imminent, immediate, and continuing.

259. As a direct and proximate result of Defendant's breach of the bailment, Plaintiff and Class Members are entitled to and do demand actual, compensatory, and punitive damages, as well as injunctive relief, and all other relief allowed by law.

COUNT XI
DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Classes)

260. Plaintiff re-alleges and incorporates the preceding paragraphs as if fully set forth herein.

261. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, the Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this complaint.

262. An actual controversy has arisen regarding Guardian's present and prospective common law and other duties to keep its Customers' Personal and Financial Information confidential and whether Defendant is currently keeping that information confidential. Plaintiff remains a Guardian Customer who needs to use the Guardian's Website to manage accounts and the financial services provided by Guardian. Plaintiff and similar Class Members thus remain at imminent risk that additional disclosure of their Personal and Financial Information will occur in the future.

263. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant continues to owe a legal duty to secure Customers' Personal and Financial Information, under the common law, Section 5 of the FTC Act, the GLBA, and various state statutes;

b. Defendant continues to breach this legal duty by disclosing its Customers' Personal and Financial Information, to unaffiliated Third Parties.

264. The Court also should issue corresponding prospective injunctive relief requiring Defendant to keep its nonpublic personal information, including Personal and Financial Information, confidential consistent with law and industry standards.

265. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury, and lack an adequate legal remedy. The risk of additional disclosure is real, immediate, and substantial, as trackers remain operative on Defendant's website to this day. If additional disclosure occurs, Plaintiff and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

266. The hardship to Plaintiff and Class Members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if Guardian continues to disclose its Customers' Personal and Financial Information, Plaintiff and Class Members will likely be subjected to the harms described herein. On the other hand, the cost to Defendant of complying with an injunction by keeping its Customers' Personal and Financial Information, confidential is relatively minimal (for example, removing trackers from its website), and Defendant has a pre-existing contractual and legal obligation to do so.

267. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing Guardian's additional unlawful disclosures of Customers' Personal and Financial Information, thus eliminating the additional injuries that would result to Plaintiff and the hundreds of thousands of Customers whose information has been and will continue to be disclosed.

COUNT XII
VIOLATION OF THE WISCONSIN DECEPTIVE TRADE PRACTICES ACT, WIS. STAT. § 100.18(1)
(On Behalf of Plaintiff and the Wisconsin Subclass)

268. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

269. The DTPA provides, in pertinent part:

> No person, firm, corporation or association, or agent or employee thereof ... with intent to induce the public in any manner to enter into any contract or obligation relating to the purchase, sale, hire, use or lease of any ... merchandise ... shall make ... an advertisement, announcement, statement or representation of any kind to the public ... which advertisement, announcement, statement or representation contains any assertion, representation or statement of fact which is untrue, deceptive or misleading.

Wis. Stat. § 100.18(1).

270. By representing that it would protect its Customers' Personal and Financial Information, Defendant made statements and representations that were untrue, deceptive, and/or misleading, as Defendant did not protect its Customers' Personal and Financial Information, and instead Disclosed it to Third Parties like Google. Defendant's deceptive acts include but are not limited to:

a. Encouraging patients to use Guardian's Website while failing to disclose the material fact that it discloses patients' Personal and Financial Information to Third Parties (and fourth parties), without authorization or permission. information relating to Plaintiff's and Class Members' financial services, without their knowledge, consent, or authorization, as part of a scheme, artifice or device with the intent to mislead patients.

b. Encouraging patients to use Guardian's Website while omitting the material fact that it uses patients' Personal and Financial Information, without their authorization for marketing purposes and to increase its revenue.

c. Marketing itself as a trusted financial services provider while failing to adhere to data privacy standards that govern financial services providers, including federal law and regulations, industry standards, and the fiduciary duties that apply to financial services providers.

d. By installing and implementing trackers from Third Parties, Defendant knew or reasonably should have known it intercepted and transmitted Plaintiff's and Class Member's communications from Plaintiff's and Class Members' browsers directly to the Third Party creators of those trackers.

271. Guardian's violations were willful and were done as part of a scheme, artifice, or device with intent to defraud or mislead, and therefore are incurable deceptive acts under the DTPA.

272. The DTPA provides a private cause of action for persons suffering a pecuniary loss as a result of a violation of the statute:

> Any person suffering pecuniary loss because of a violation of this section by any other person may sue in any court of competent jurisdiction and shall recover such pecuniary loss, together with costs, including reasonable attorney fees.

Wis. Stat. § 100.18(11)(b).

273. Had Plaintiff and members of the Wisconsin subclass been aware that their Personal and Financial Information would be transmitted to unauthorized third parties, they would not have entered into such transactions and would not have provided payment or confidential financial information to Defendant.

274. As a direct and proximate result of Defendant's unfair and deceptive acts and practices in violation of the DTPA, Plaintiff and Class Members have suffered damages for which Defendant is liable.

275. Plaintiff and Class Members seek actual damages plus interest on damages at the legal rate, as well as all other just and proper relief afforded by the DTPA. As redress for Defendant's repeated and ongoing violations, Plaintiff and Class Members are entitled to, inter alia, actual damages, treble damages, attorneys' fees, and injunctive relief.

COUNT XIII
VIOLATION OF THE WISCONSIN CONSUMER PROTECTION ACT, WIS. STAT. § 422.503
(On Behalf of Plaintiff and the Wisconsin Subclass)

276. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

277. The WCPA § 422.503 sets forth prohibited activities by a credit services organization. The act provides, in pertinent part:

> A credit services organization, and its salespersons, agents and representatives who offer or sell the services of the credit services organization, may not…Make or use any untrue or misleading representations in the offer or sale of the services of the credit services organization or engage, directly or indirectly, in any act, practice or course of business that operates or would operate as a fraud or deception upon any person in connection with the offer or sale of the services of a credit services organization.

Wis. Stat. § 423.301.

278. Defendant is a credit services organization as defined under Wisconsin statute.

279. By representing, in connection with the offer or sale of its credit services, that it would protect its Customers' Personal and Financial Information, Defendant made statements and representations that were untrue, deceptive, and/or misleading, operating as a fraud or deception upon Plaintiff and Class Members. Defendant did not protect its Customers' Personal and Financial Information, and instead Disclosed it to Third Parties like Google. Defendant made these representations with regard to the extension of consumer credit, specifically with respect to the terms or conditions for the extension of that credit. Defendant's deceptive acts include but are not limited to:

a. Encouraging patients to use Guardian's Website while failing to disclose the material fact that it discloses patients' Personal and Financial Information to Third Parties (and fourth parties), without authorization or permission. information relating to Plaintiff's and Class Members' financial services, without their knowledge, consent, or authorization, as part of a scheme, artifice or device with the intent to mislead patients.

b. Encouraging patients to use Guardian's Website while omitting the material fact that it uses patients' Personal and Financial Information, without their authorization for marketing purposes and to increase its revenue.

c. Marketing itself as a trusted financial services provider while failing to adhere to data privacy standards that govern financial services providers, including federal law and regulations, industry standards, and the fiduciary duties that apply to financial services providers.

d. By installing and implementing trackers from Third Parties, Defendant knew or reasonably should have known it intercepted and transmitted Plaintiff's and Class Member's communications from Plaintiff's and Class Members' browsers directly to the Third Party creators of those trackers.

280. Guardian's violations were willful and were done as part of a scheme, artifice, or device with intent to defraud or mislead, and therefore are incurable deceptive acts under the WCPA.

281. Had Plaintiff and members of the Wisconsin subclass been aware that their Personal and Financial Information would be transmitted to unauthorized third parties, they would not have

entered into such transactions and would not have provided payment or confidential financial information to Defendant.

282. As a direct and proximate result of Defendant's unfair and deceptive acts and practices in violation of the WCPA, Plaintiff and Class Members have suffered damages for which Defendant is liable.

283. Plaintiff and Class Members seek actual damages plus interest on damages at the legal rate, as well as all other just and proper relief afforded by the WCPA. As redress for Defendant's repeated and ongoing violations, Plaintiff and Class Members are entitled to, inter alia, actual damages, treble damages, attorneys' fees, and injunctive relief.

COUNT XIV
VIOLATION OF THE WISCONSIN CONSUMER PROTECTION ACT, WIS. STAT. § 423.301
(On Behalf of Plaintiff and the Wisconsin Subclass)

284. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

285. The WCPA § 423.301 was designed to impede false, misleading, and deceptive statements relating to the extension of consumer credit. The act provides, in pertinent part:

> No merchant shall advertise, print, display, publish, distribute or broadcast or cause to be advertised, printed, displayed, published, distributed or broadcast, in any manner any statement or representation with regard to the extension of consumer credit including the rates, terms or conditions for the extension of such credit, which is false, misleading, or deceptive, or which omits to state material information with respect to the extension of credit that is necessary to make the statements therein not false, misleading or deceptive.

Wis. Stat. § 423.301.

286. By representing that it would protect its Customers' Personal and Financial Information, Defendant made statements and representations that were untrue, deceptive, and/or misleading, as Defendant did not protect its Customers' Personal and Financial Information, and instead Disclosed it to Third Parties like Google. Defendant made these representations with regard

to the extension of consumer credit, specifically with respect to the terms or conditions for the extension of that credit. Defendant's deceptive acts include but are not limited to:

a. Encouraging patients to use Guardian's Website while failing to disclose the material fact that it discloses patients' Personal and Financial Information to Third Parties (and fourth parties), without authorization or permission. information relating to Plaintiff's and Class Members' financial services, without their knowledge, consent, or authorization, as part of a scheme, artifice or device with the intent to mislead patients.

b. Encouraging patients to use Guardian's Website while omitting the material fact that it uses patients' Personal and Financial Information, without their authorization for marketing purposes and to increase its revenue.

c. Marketing itself as a trusted financial services provider while failing to adhere to data privacy standards that govern financial services providers, including federal law and regulations, industry standards, and the fiduciary duties that apply to financial services providers.

d. By installing and implementing trackers from Third Parties, Defendant knew or reasonably should have known it intercepted and transmitted Plaintiff's and Class Member's communications from Plaintiff's and Class Members' browsers directly to the Third Party creators of those trackers.

287. Guardian's violations were willful and were done as part of a scheme, artifice, or device with intent to defraud or mislead, and therefore are incurable deceptive acts under the WCPA.

288. Had Plaintiff and members of the Wisconsin subclass been aware that their Personal and Financial Information would be transmitted to unauthorized third parties, they would not have entered into such transactions and would not have provided payment or confidential financial information to Defendant.

289. As a direct and proximate result of Defendant's unfair and deceptive acts and practices in violation of the WCPA, Plaintiff and Class Members have suffered damages for which Defendant is liable.

290. Plaintiff and Class Members seek actual damages plus interest on damages at the legal rate, as well as all other just and proper relief afforded by the WCPA. As redress for Defendant's repeated and ongoing violations, Plaintiff and Class Members are entitled to, inter alia, actual damages, treble damages, attorneys' fees, and injunctive relief.

COUNT XV
MISAPPROPRIATION OF AN INDIVIDUAL'S PERSONAL IDENTIFYING INFORMATION, WIS. STAT. § 943.201
(On Behalf of Plaintiff and the Wisconsin Subclass)

291. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

292. The state of Wisconsin makes it a crime to "obtain credit, money, goods, services, employment, or any other thing of value or benefit" by stealing someone's personal identifying information. Wis. Stat. § 943.201.

293. The Wisconsin offense occurs when a person "intentionally uses, attempts to use, or possesses with intent to use any personal identifying information or personal identification document of an individual ... without the[ir] authorization or consent ... [t]o obtain credit, money, goods, services, employment, or any other thing of value or benefit." Wis. Stat. § 943.201(2)(a).

294. Personally identifying information can include an individual's name, address, telephone number, or any other "information or data that is unique to, assigned to, or belongs to

an individual and that is intended to be used to access services, funds, or benefits of any kind to which the individual is entitled." Wis. Stat. § 943.201(1)(b).

295. Defendant used Plaintiff and Class Members' personal identifying information without their consent. At no time did Plaintiff or Class Members consent to Defendant's use of their Personal and Financial Information for sale and marketing purposes.

296. Defendant collected, used, and disclosed this information to obtain a thing of value or benefit for its own gain, for marketing purposes, and for sale or trade with Third Parties. Defendant did not share this benefit with Plaintiff and Class Members.

297. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiff and Class Members.

298. Plaintiff and Class Members would not have used Defendant's services, or would have paid less for those services, if they had known that Defendant would collect, use, and disclose their Personal and Financial Information to Third Parties or allow Third Parties (and fourth parties) to use their Personal and Financial Information.

299. Had Plaintiff and members of the Wisconsin subclass been aware that their Personal and Financial Information would be transmitted to unauthorized third parties, they would not have entered into such transactions and would not have provided payment or confidential financial information to Defendant.

300. "Any person who suffers damage or loss" as a result of a violation of Wis. Stat. § 943.201 "has a cause of action against the person who caused the damage or loss." Wis. Stat. § 895.446(1).

301. Plaintiff and Class Members are entitled to actual damages, costs of investigation and litigation, and exemplary damages of three times the actual damages.

COUNT XVI
VIOLATION OF WISCONSIN'S ELECTRONIC SURVEILLANCE CONTROL LAW, WIS. STAT. § 968.27, *ET SEQ.*
(On Behalf of Plaintiff and the Wisconsin Subclass)

302. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

303. Under Wisconsin's Electronic Surveillance Control Law ("ESCL"):

> whoever commits any of the acts enumerated in this section is guilty of a Class H felony:
>
> (a) Intentionally intercepts, attempts to intercept or procures any other person to intercept or attempt to intercept, any wire, electronic or oral communication.
>
> (b) Intentionally uses, attempts to use or procures any other person to use or attempt to use any electronic, mechanical or other device to intercept any oral communication.
>
> (c) Discloses, or attempts to disclose, to any other person the contents of any wire, electronic or oral communication, knowing or having reason to know that the information was obtained through the interception of a wire, electronic or oral communication in violation of this section or under circumstances constituting violation of this section.
>
> (d) Uses, or attempts to use, the contents of any wire, electronic or oral communication, knowing or having reason to know that the information was obtained through the interception of a wire, electronic or oral communication in violation of this section or under circumstances constituting violation of this section.
>
> (e) Intentionally discloses the contents of any oral, electronic or wire communication obtained by authority of ss. 968.28, 968.29 and 968.30, except as therein provided.
>
> (f) Intentionally alters any wire, electronic or oral communication intercepted on tape, wire or other device.

Wis. Stat. Ann. § 968.31.

304. For purposes of the ESCL, "'Electronic communication' means any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature wholly or partially transmitted by a wire, radio, electromagnetic, photoelectronic or photooptical system." Wis. Stat. Ann. § 968.27 (4).

305. "'Electronic, mechanical or other device' means any device or apparatus which can be used to intercept a wire, electronic or oral communication." Wis. Stat. Ann. § 968.27(7).

306. "'Intercept' means the aural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device." Wis. Stat. Ann. § 968.27(9).

307. "It is not unlawful … For a person not acting under color of law to intercept a wire, electronic or oral communication where the person is a party to the communication or where one of the parties to the communication has given prior consent to the interception **unless the communication is intercepted for the purpose of committing any criminal or tortious act in violation of the constitution or laws of the United States or of any state or for the purpose of committing any other injurious act**." Wis. Stat. Ann. § 968.31(2)(c) (emphasis added)

308. Defendant intentionally recorded and/or acquired Plaintiff's and Class Members' private electronic communications, without the consent of Plaintiff and Class Members, using Google Trackers and similar tracking technologies on its Website.

309. Defendant intentionally recorded and/or acquired Plaintiff's and Class Members' private electronic communications for the purpose of disclosing those communications to Third Parties (and Fourth Parties), including Google, without the knowledge, consent, or written authorization of Plaintiff or Class Members.

310. Plaintiff's and Class Members' communications with Defendant constitute private conversations, communications, and information.

311. Plaintiff and Class Members had a reasonable expectation of privacy in their communications with Defendant via its Website.

312. Plaintiff and Class Members communicated sensitive Personal and Financial Information that they intended for only Defendant to receive and that they understood Defendant would keep private.

313. Plaintiff and Class Members have a reasonable expectation that Defendant would not disclose Personal and Financial Information and confidential communications to Third Parties (and Fourth Parties) without Plaintiff's or Class Members' authorization, consent, or knowledge.

314. Plaintiff and Class Members had a reasonable expectation of privacy given Defendant's representations, Privacy Policies, and state and federal law. Moreover, Plaintiff and Class Members have a general expectation that their communications regarding financial services with their financial services providers will be kept confidential.

315. Plaintiff and Class Members were unaware that their Personal and Financial Information was being surreptitiously recorded and transmitted to third parties as they communicated with Defendant through its Online Platforms.

316. Without Plaintiff's or Class Members' knowledge, authorization, or consent, Defendant used the Google tracker imbedded and concealed into the source code of its Website to secretly record and transmit Plaintiff's and Class Members' private communications to hidden Third Parties, such as Google, as described in the preceding paragraphs.

317. Defendant's Disclosure of Plaintiff's and Class Members' Personal and Financial Information was for the purpose of committing a criminal or tortious act in violation of a variety of laws, as set forth throughout this complaint.

318. Under the ESCL:

> Any person whose wire, electronic or oral communication is intercepted, disclosed or used in violation of ss. 968.28 to 968.37 shall have a civil cause of action against any person who intercepts, discloses or uses, or procures any other person to

intercept, disclose, or use, the communication, and shall be entitled to recover from any such person:

(a) Actual damages, but not less than liquidated damages computed at the rate of $100 a day for each day of violation or $1,000, whichever is higher;
(b) Punitive damages; and
(c) A reasonable attorney's fee and other litigation costs reasonably incurred

Wis. Stat. Ann. § 968.31(2m).

319. The eavesdropping devices used in this case include, but are not limited to:

a. Plaintiff's and Class Members' personal computing devices;

b. Plaintiff's and Class Members' web browsers;

c. Plaintiff's and Class Members' browser-managed files;

d. Google's trackers;

e. Internet cookies;

f. Other tracking technology including LinkedIn, Qualtrics, and Adnxs;

g. Defendant's computing servers;

h. Third-party source code utilized by Defendant; and

i. Computer servers of third-parties (including Google) to which Plaintiff's and Class Members' communications were disclosed.

320. Defendant aided in the interception of communications between Plaintiff and Class Members and Defendant that were redirected to and recorded by third parties without Plaintiff's or Class Members' consent.

321. Under the ESCL, Plaintiff and the Class Members are entitled to injunctive relief prohibiting further eavesdropping by Defendant, actual damages, and punitive damages.

322. Defendant's violation of the ESCL caused Plaintiff and Class Members the following damages:

a. Sensitive and confidential information that Plaintiff and Class Members intended to remain private is no longer private;

b. Defendant eroded the essential confidential nature of the relationship a Customer has with their financial institution;

c. Defendant took something of value from Plaintiff and Class Members and derived benefit therefrom without Plaintiff's and Class Members' knowledge or informed consent and without sharing the benefit of such value;

d. Plaintiff and Class Members did not get the full value of the financial services for which they paid, which included Defendant's duty to maintain confidentiality; and

e. Defendant's actions diminished the value of Plaintiff's and Class Members' Personal and Financial Information.

323. Plaintiff and Class Members also seek such other relief as the Court may deem equitable, legal, and proper.

COUNT XVII
VIOLATION OF WISCONSIN'S ELECTRONIC SURVEILLANCE CONTROL LAW, WIS. STAT. § 968.34, *ET SEQ.*
(On Behalf of Plaintiff and the Wisconsin Subclass)

324. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

325. Under the ESCL, "no person may install or use a pen register or a trap and trace device without first obtaining a court order." Wis. Stat. Ann. § 968.34.

326. The ESCL defines a "pen register" as "a device that records or decodes electronic or other impulses that identify the numbers dialed or otherwise transmitted on the telephone line to which the device is attached." Wis. Stat. Ann. § 968.27(13).

327. The tracking technologies Defendant installed on its Website constitute a "pen register" because they record information—Plaintiff and Class Members' Personal and Financial

Information including their identifying information and location data-from the electronic communications transmitted on Defendant's Website.

328. Defendant was not authorized by any court order to use a pen register to track Plaintiff's and Class Members' location data and personal information.

329. Defendant did not have Plaintiff or Class Members' consent to use a pen register.

330. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members suffered losses and were damaged in an amount to be determined at trial.

331. Under the ESCL:

> Any person whose wire, electronic or oral communication is intercepted, disclosed or used in violation of ss. 968.28 to 968.37 shall have a civil cause of action against any person who intercepts, discloses or uses, or procures any other person to intercept, disclose, or use, the communication, and shall be entitled to recover from any such person:
>
> (a) Actual damages, but not less than liquidated damages computed at the rate of $100 a day for each day of violation or $1,000, whichever is higher;
> (b) Punitive damages; and
> (c) A reasonable attorney's fee and other litigation costs reasonably incurred

Wis. Stat. Ann. § 968.31(2m).

332. Defendant's violation of the ESCL caused Plaintiff and Class Members the following damages:

a. Sensitive and confidential information that Plaintiff and Class Members intended to remain private is no longer private;

b. Defendant eroded the essential confidential nature of the relationship a Customer has with their financial institution;

c. Defendant took something of value from Plaintiff and Class Members and derived benefit therefrom without Plaintiff's and Class Members' knowledge or informed consent and without sharing the benefit of such value;

d. Plaintiff and Class Members did not get the full value of the financial services for which they paid, which included Defendant's duty to maintain confidentiality; and

e. Defendant's actions diminished the value of Plaintiff's and Class Members' Personal and Financial Information.

333. Plaintiff and Class Members also seek such other relief as the Court may deem equitable, legal, and proper.

COUNT XVIII
VIOLATION OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT
18 U.S.C. §§ 2511(1), ET SEQ.
(On Behalf of Plaintiff and the Classes)

334. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

335. The ECPA protects both sending and receipt of communications. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

336. The transmissions of Plaintiff's and Class Members' Personal and Financial Information to Defendant's Website qualifies as a "communication" under the ECPA's definition of 18 U.S.C. § 2510(12).

337. **Electronic Communications**. The transmission of Personal and Financial Information between Plaintiff and Class Members and Defendant's Website with which they chose to exchange communications are "transfer[s] of signs, signals, writing,…data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photo optical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(2).

338. **Content**. The ECPA defines content, when used with respect to electronic communications, to "include [] any information concerning the substance, purport, or meaning of that communication." *See* 18 U.S.C. § 2510(8).

339. **Interception**. The ECPA defines the interception as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device" and "contents…include any information concerning the substance, purport, or meaning of that communication." See 18 U.S.C. § 2510(4), (8).

340. **Electronic, Mechanical or Other Device**. The ECPA defines "electronic, mechanical, or other device" as "any device…which can be used to intercept a[n]…electronic communication[.]" 18 U.S.C. § 2510(5). The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a. Plaintiff's and Class Members' browsers;

b. Plaintiff's and Class Members' computing devices;

c. Defendant's web-servers;

d. Defendant's Website; and

e. The tracking technology deployed by Defendant effectuated the sending and acquisition of customer communications.

341. By utilizing and embedding the tracking technology on its Website, Defendant intentionally intercepted, endeavored to intercept and procured another person to intercept the electronic communications of Plaintiff and Class Members, in violation of 18 U.S.C. § 2511(1)(a).

342. Specifically, Defendant intercepted Plaintiff's and Class Members' electronic communications via the tracking technology which tracked, stored, and unlawfully disclosed Plaintiff's and Class Members' Personal and Financial Information to Third Parties.

343. Defendant's intercepted communications include, but are not limited to, communications to/from Plaintiff and Class Members regarding Personal and Financial Information.

344. By intentionally disclosing or endeavoring to disclose the electronic communications of Plaintiff and Class Members to Third Parties, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

345. By intentionally using, or endeavoring to use, the contents of the electronic communications of Plaintiff and Class Members, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

346. **Unauthorized Purpose.** Defendant intentionally intercepted the contents of Plaintiff's and Class Members' electronic communications for the purpose of committing a tortious act in violation of the Constitution or laws of the United States or of any State – namely, invasion of privacy, among others.

347. Defendant intentionally used the wire or electronic communications to increase its profit margins and save on marketing costs.

348. Defendant specifically used tracking technology to track and to utilize Plaintiff's and Class Members' Personal and Financial Information for financial gain.

349. Defendant was not acting under color of law to intercept Plaintiff's and Class Members' wire or electronic communication.

350. Plaintiff and Class Members did not authorize Defendant to acquire the content of their communications for purposes of invading Plaintiff's and Class Members' privacy via the tracking technology.

351. In sending and in acquiring the content of Plaintiff's and Class Members' communications relating to the browsing of its Website, Defendant's purpose was tortious, criminal and designed to violate federal and state legal provisions, including as described above the following: (i) a knowing intrusion into a private, place, conversation or matter that would be highly offensive to a reasonable person; and (ii) violation of GLBA, the FTC Act, invading Plaintiff's and Class Members' privacy, and in breach of its fiduciary duty of confidentiality.

COUNT XIX
VIOLATION OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT
18 U.S.C. § 2511(3)(A)
UNAUTHORIZED DIVULGENCE BY ELECTRONIC COMMUNICATIONS SERVICE
(On Behalf of Plaintiff and the Classes)

352. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

353. The ECPA provides that "a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient." 18 U.S.C. § 2511(3)(a).

354. **Electronic Communication Service**. An "electronic communication service" is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). Defendant's Website is an electronic communication service which provides to users thereof, customers of Defendant, the ability to send or receive electronic communications; in the absence of Defendant's Website, internet users

could not send or receive communications regarding Plaintiff's and Class Members' Personal and Financial Information.

355. **Intentional Divulgence**. Defendant intentionally designed the tracking technology and was or should have been aware that, if so configured, it could divulge Plaintiff's and Class Members' Personal and Financial Information. Upon information and belief, Defendant's divulgence of the contents of Plaintiff's and Class Members' communications was contemporaneous with their exchange with Defendant's Website, to which they directed their communications.

356. Defendant divulged the contents of Plaintiff's and Class Members' electronic communications without authorization and/or consent.

357. **Exceptions do not apply**. In addition to the exception for communications directly to an electronic communications service ("ECS")[52] or an agent of an ECS, the ECPA states that

> A person or entity providing electronic communication service to the public may divulge the contents of any such communication—
>
> (i) as otherwise authorized in section 2511(2)(a) or 2517 of this title;
>
> (ii) with the lawful consent of the originator or any addressee or intended recipient of such communication;
>
> (iii) to a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or
>
> (iv) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.

U.S.C. § 2511(3)(b).

358. Section 2511(2)(a)(i) provides:

> It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal

[52] An ECS is "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

> course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

359. Defendant's divulgence of the contents of Plaintiff's and Class Members' communications to Third Parties was not authorized by 18 U.S.C. § 2511(2)(a)(i) in that it was neither: (i) a necessary incident to the rendition of Defendant's service nor (ii) necessary to the protection of the rights or property of Defendant.

360. Section 2517 of the ECPA relates to investigations by government officials and has no relevance here.

361. Defendant's divulgence of the contents of Plaintiff's and the Class Members' communications on its Website through the tracking technology was not done "with the lawful consent of the originator or any addresses or intended recipient of such communication[s]." 18 U.S.C.A. § 2511(3)(b)(ii). As alleged above: (i) Plaintiff and Class Members did not authorize Defendant to divulge the contents of their communications and (ii) Defendant did not procure the "lawful consent" from the websites or apps with which Plaintiff and Class Members were exchanging information.

362. Moreover, Defendant divulged the contents of Plaintiff's and Class Members' communications through tracking technology to individuals who are not "person[s] employed or whose facilities are used to forward such communication to its destination."

363. The contents of Plaintiff's and Class Members' communications did not appear to pertain to the commission of a crime and Defendant did not divulge the contents of their communications to a law enforcement agency.

364. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages, preliminary and other equitable or declaratory relief as may be appropriate, punitive damages in an amount to be determined by a jury and a reasonable attorney's fee and other litigation costs reasonably incurred.

COUNT XX
VIOLATION OF TITLE II OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT ("STORED COMMUNICATIONS ACT")
18 U.S.C. § 2702, ET SEQ.
(On Behalf of Plaintiff and the Classes)

365. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

366. The ECPA further provides that "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." 18 U.S.C. § 2702(a)(1).

367. **Electronic Communication Service**. ECPA defines "electronic communications service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). Defendant intentionally procures and embeds various Plaintiff's and Class Members' Personal and Financial Information through the tracking technology used on Defendant's Website, which qualifies as an Electronic Communication Service.

368. **Electronic Storage**. ECPA defines "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17).

369. Defendant stores the content of Plaintiff's and Class Members' communications on Defendant's Website and files associated with it.

370. When Plaintiff or Class Members make a Website communication, the content of that communication is immediately placed into storage.

371. Defendant knowingly divulges the contents of Plaintiff's and Class Members' communications through the tracking technology.

372. **Exceptions Do Not Apply**. Section 2702(b) of the Stored Communication Act provides that an electronic communication service provider

> may divulge the contents of a communication—
> (1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;
> (2) as otherwise authorized in Section 2517, 2511(2)(a), or 2703 of this title;
> (3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;
> (4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;
> (5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;
> (6) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A;
> (7) to a law enforcement agency—
> (A) if the contents—
> (i) were inadvertently obtained by the service provider; and
> (ii) appear to pertain to the commission of a crime; . . .
> (8) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency; or
> (9) to a foreign government pursuant to an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies Section 2523.

373. Defendant did not divulge the contents of Plaintiff's and Class Members' communications to "addressees," "intended recipients," or "agents" of any such addressees or intended recipients of Plaintiff and Class Members.

374. Sections 2517 and 2703 of the ECPA relate to investigations by government officials and have no relevance here.

375. Section 2511(2)(a)(i) provides:

> It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

376. Defendant's divulgence of the contents of Plaintiff's and Class Members' communications on its Website to Third Parties was not authorized by 18 U.S.C. § 2511(2)(a)(i) in that it was neither: (i) a necessary incident to the rendition of the Defendant's services nor (ii) necessary to the protection of the rights or property of Defendant.

377. Defendant's divulgence of the contents of Plaintiff's and Class Members' customer user communications on its Website was not done "with the lawful consent of the originator or any addresses or intended recipient of such communication[s]." 18 U.S.C.A. § 2511(3)(b)(ii). As alleged above: (i) Plaintiff and Class Members did not authorize Defendant to divulge the contents of their communications and (ii) Defendant did not procure the "lawful consent" from the websites or apps with which Plaintiff and Class Members were exchanging information.

378. Moreover, Defendant divulged the contents of Plaintiff's and Class Members' communications through the tracking technology to individuals who are not "person[s] employed or whose facilities are used to forward such communication to its destination."

379. The contents of Plaintiff's and Class Members' communications did not appear to pertain to the commission of a crime and Defendant did not divulge the contents of their communications to a law enforcement agency.

380. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages, preliminary and other equitable or declaratory relief as may be

appropriate, punitive damages in an amount to be determined by a jury and a reasonable attorney's fee and other litigation costs reasonably incurred.

COUNT XXI
VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT ("CFAA")
18 U.S.C. § 1030, ET SEQ.
(On Behalf of Plaintiff and the Classes)

381. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

382. Plaintiff's and the Class Members' computers and mobile devices are, and at all relevant times have been, used for interstate communication and commerce, and are therefore "protected computers" under 18 U.S.C. § 1030(e)(2)(B).

383. Defendant exceeded, and continues to exceed, authorized access to Plaintiff's and the Class Members' protected computers and obtained information thereby, in violation of 18 U.S.C. § 1030(a)(2), (a)(2)(C).

384. Defendant's conduct caused "loss to 1 or more persons during any 1-year period… aggregating at least $5,000 in value" under 18 U.S.C. § 1030(c)(4)(A)(i)(I), *inter alia*, because of the secret transmission of Plaintiff's and the Class Members' Personal and Financial Information as set forth in detail herein, which were never intended for public consumption.

385. Defendant's conduct also constitutes "a threat to public health or safety" under 18 U.S.C. § 1030(c)(4)(A)(i)(IV), due to the private and personally identifiable data and content of Plaintiff and the Class Members' Personal and Financial Information and communication being made available to Defendant and Third Parties without adequate legal privacy protections.

386. Accordingly, Plaintiff and the Class Members are entitled to "maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." 18 U.S.C. § 1030(g).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually, on behalf of himself and all others similarly situated, prays for judgment as follows:

A. For an Order certifying this action as a Class action and appointing Plaintiff as Class Representatives and Plaintiff's counsel as Class Counsel;

B. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

C. For an award of punitive damages, as allowable by law;

D. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Personal and Financial Information and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

E. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety and to disclose with specificity the type of Personal and Financial Information compromised and unlawfully disclosed to Third Parties;

F. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

G. For an Order compelling Defendant to pay for not less than three years of credit monitoring services for Plaintiff and the Classes;

H. For an award of reasonable attorneys' fees and costs under the laws outlined above, the common fund doctrine, and any other applicable law;

I. Costs and any other expenses, including expert witness fees incurred by Plaintiff in connection with this action;

J. Pre- and post-judgment interest on any amounts awarded; and

K. Such other and further relief as this court may deem just and proper.

JURY DEMAND

Plaintiff, on behalf of himself, and all others similarly situated, hereby demands a trial by jury on all issues so triable.

Dated: February 4, 2025

Respectfully submitted,

/s/Samuel J. Strauss

Samuel J. Strauss (WI Bar #1113942)
Raina C. Borrelli*
STRAUSS BORRELLI, PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, Indiana 60611
(872) 263-1100
(872) 263-1109 (facsimile)
sam@straussborrelli.com
raina@straussborrelli.com

Lynn A. Toops*
Amina A. Thomas*
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, Indiana 46204
(317) 636-6481
ltoops@cohenandmalad.com
athomas@cohenandmalad.com

J. Gerard Stranch, IV*
Emily E. Schiller*
STRANCH, JENNINGS & GARVEY, PLLC
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 37203
(615) 254-8801
(615) 255-5419 (facsimile)
gstranch@stranchlaw.com

eschiller@stranchlaw.com

* to seek admission *pro hac vice*

Counsel for Plaintiff and the Proposed Classes